

# **The Legal Nature of Digital Assets**

Hin Liu

(廖衍廷)

Linacre College

**Degree:** Doctor of Philosophy in Law

**Word count:** 102,343

**Term Submitted:** Hilary Term 2025

**Supervisors:** Luke Rostill and Ben McFarlane

**Title of thesis:** The Legal Nature of Digital Assets

**Name of candidate:** Hin Ting Liu

**College:** Linacre College

**Degree:** DPhil in Law

**Term and year of submission:** Hilary Term 2025

***Abstract.*** This thesis explores the legal nature of digital assets from the perspective of property law. It discusses four questions that have been underexplored in the case law and literature in relation to digital assets: (1) the conceptual capability and normative desirability of recognising property rights in respect of digital assets; (2) when a property right in a digital asset ought to be acquired for the first time; (3) when one ought to be able to transfer such a right; and (4) the strength of such a right against third parties generally.

It argues, in relation to (1), that it is conceptually possible and normatively desirable to recognise property rights (in the sense of non-interference rights effective against the world) in respect of a digital asset. In relation to (2), an original property right should arise where one has positive and negative control of a digital asset plus an intention to exercise control over it on one's own behalf. In relation to (3), the right should be transferred only when there is a change of control plus an intention to transfer the right. Finally, in relation to (4), the current law leaves a gap in protection in respect of digital assets, and it should not be filled by extending the chattel torts to them, but should rather be addressed by a new regime that (i) provides a remedy where one's use of their digital asset has been intentionally or recklessly impaired, and (ii) allows one to recover control of a digital asset from a person with no property right or an inferior property right in it.

## Table of Contents

Table of Abbreviations.....	vii
Table of Cases.....	viii
Table of Statutes.....	xiv
Table of Other Primary Legal Sources.....	xviii

### **Introduction** ..... 1

1. Background.....	1
2. Focus of this thesis, and importance of its contribution.....	10
2.1 Aim, substance, and technique.....	12
2.2 State of the case law, commentary, and legislation, and what ‘gap’ is to be filled.....	14
2.3 Structure of thesis.....	18

### **Chapter 1: Digital Assets as Property?** ..... 19

1. Introduction.....	19
2. Meaning of ‘digital asset’.....	19
2.1 Types of digital assets.....	21
2.2 Summary of digital assets explored in thesis.....	24
3. Meaning of ‘property’.....	24
3.1 Meaning 1: Realisable commercial value.....	25
3.2 Meaning 2: Non-interference rights .....	25
3.3 Meaning 3: Non-interference rights plus powers.....	28
3.4 Meaning 4: Satisfying the conditions in <i>Ainsworth</i> .....	30
3.5 Meaning 5: Insolvency.....	31
4. Non-interference rights.....	33
4.1 Meaning 2 v Meaning 3.....	33
4.2 Meaning 2 v Meaning 5.....	36
4.3 Discussion of title, ownership, and the right to exclude.....	37

4.3.1 Title and ownership.....	37
4.3.2 The ‘right to exclude’.....	39
5. The case law.....	39
5.1 Interim applications cases.....	40
5.2 Insolvency cases.....	44
5.3 Miscellaneous contract and trust cases.....	47
5.4 Gap in the case law.....	50
6. Whether digital assets are conceptually capable of constituting property, and the normative case.....	52
6.1 Features of digital assets in more detail.....	52
6.1.1 Notional quantity unit + Data entries and software.....	53
6.1.2 ‘Rivalrous’.....	54
6.1.3 ‘Independent of the legal system and other persons’.....	55
6.1.4 Digital assets as physical assets? .....	55
6.2 Conceptual capability of constituting property.....	57
6.2.1 Some differences from other types of rights.....	60
6.2.2 Potential content of the property right.....	64
6.2.2.1 Position 1: Right that others not interfere with a thing.....	65
6.2.2.2 Position 2: Right to exclusive control.....	67
6.2.2.3 Position 3: Right to exclude others from use, occupancy and possession.....	68
6.2.2.4 Position 4: Right that others not impair use of asset intentionally or recklessly, plus right to recover control of asset.....	69
6.2.2.5 Position 5: Right that others not impair usability of asset.....	70
6.2.2.6 Taking stock.....	71
6.3 The normative case.....	72
6.3.1 The basic argument: giving effect to expectations.....	72
6.3.2 Higher risk of a free-for-all.....	75
7. Conclusion.....	81
 <b>Chapter 2: Acquisition of a property right.....</b>	 <b>83</b>
1. Introduction.....	83

2. The normative question.....	84
2.1 Property rights to digital and physical assets.....	84
2.1.1 The ‘core’ case, and positive and negative control.....	85
2.1.1.1 Multi-signature addresses.....	88
2.1.1.2 Theft.....	91
2.1.1.3 Boundary issues.....	91
2.1.2 The intention requirement.....	93
2.2 Justifications for conferring title.....	95
2.2.1 Free-for-all.....	96
2.2.2 Limitation periods.....	97
2.2.3 Conventions and expectations.....	99
2.2.4 Other ‘general’ justifications.....	103
2.2.5 Specific v general intention.....	104
3. The doctrinal question: possession or control? .....	108
3.1 Possession and its context.....	110
3.1.1 Scope of ‘possession’ .....	113
3.1.2 The ‘general property interest’ .....	115
3.2 Possession should not be extended to digital assets.....	117
3.2.1 The possession rules are messy/unsatisfactory.....	117
3.2.1.1 Bailment.....	117
3.2.1.2 The ‘right to immediate possession’ .....	121
3.2.1.2.1 When the right to sue is lost.....	122
3.2.1.2.2 Content of a chattel lease.....	124
3.2.1.2.3 Language of ‘right to immediate possession’ .....	127
3.2.1.2.4 Starting afresh, and the numerus clausus.....	129
3.2.2 Differences between physical and digital assets.....	130
3.2.2.1 Errors in applying the ‘right to immediate possession’ concept.....	132
3.2.2.2 Effects on the physical asset threshold.....	135
3.2.3 An ‘on-off’ switch? .....	137
3.2.4 Practical effects in the litigation context.....	138
3.3 Control.....	139
3.3.1 The concept and meanings of control.....	139
3.3.2 Advantage of using control over possession.....	142

3.3.3 Why not any other concept? .....	147
4. Conclusion.....	149

**Chapter 3: Transferring the property right.....150**

1. Introduction.....	150
2. Clarification about ‘transfer’ .....	153
3. Transferring a property right: the policies.....	154
3.1 The control-title inference and decoupling.....	156
3.2 Frustration of reasonable expectations: Purchasers and creditors.....	157
3.3 Risk of fraud and misappropriation.....	158
3.4 Party autonomy.....	159
4. Ways of transferring a property right: the options.....	160
5. Deed.....	161
6. Delivery and sale: the rationales.....	163
7. Agreement.....	165
8. Change of control.....	167
8.1 The ‘change of control’ requirement and its benefits.....	168
8.1.1 Less room to fraudulently represent, and less room to be misled by control-title inference.....	169
8.1.2 Preventing fraudulent assertion and denial where no change of control.....	171
8.1.3 Similarity with delivery.....	171
8.1.4 Mental element.....	172
8.2 How much control? .....	173
8.3 Types of control.....	177
8.3.1 (Factual) positive versus negative control.....	178
8.3.2 Sole control.....	179
8.3.3. Control lost by transferor v control gained by transferee.....	180
8.3.4 Condition precedent and condition subsequent.....	181
8.3.5 Immediate control.....	183
8.3.6 Consent-based conditions.....	183
8.3.7 Avoiding false analogies or distinctions: practical examples.....	184
8.4 The linguistic formulation.....	187

8.5 The three-stage approach.....	191
9. On-chain transfer.....	192
9.1 Party autonomy.....	192
9.2 On-chain transfer to self.....	193
9.3 The ‘register’ justification.....	193
9.4 Protection of secured creditors? .....	198
9.5 Summary.....	199
10. Conclusion.....	199

## **Chapter 4: Protection against interference.....201**

1. Introduction.....	201
1.1 Structure of chapter.....	202
2. The gap in protection.....	203
2.1 The ‘core situations’ of interference.....	203
2.2 Liability for intentional misappropriation, burning or freezing.....	205
2.2.1 The conduct element.....	205
2.2.2 The mental element.....	206
2.3 The current law leaves gaps in protection.....	207
2.4 How big is the gap? .....	210
2.5 Filling the gap.....	212
3. Option 1: Extending the chattel torts.....	212
3.1 The argument in favour of extending the chattel torts.....	213
3.2 The three reasons why the chattel torts should not be extended to digital assets.....	215
3.3 The interference regime for physical assets.....	217
3.3.1 Elements 1 and 2: Action of the defendant and impact on the claimant’s asset or use of his asset.....	218
3.3.2 Element 3: Proximity/causation.....	221
3.3.3 Element 4: Mental requirement.....	222
3.3.4 Element 5: Defences.....	223
3.4 Argument 1: Difficulty in applying chattel tort elements and normative balance to digital assets.....	223
3.4.1 No proxy for physical interference.....	226

3.4.2 Blockchain environment/policy (v physical environment/policy).....	232
3.5 Argument 2: Chattel tort rules themselves are unsatisfactory and arguably too harsh.....	237
3.5.1 ‘Right to immediate possession’ .....	237
3.5.2 Definitions and formulations of conversion.....	239
3.5.3 Strict liability.....	241
3.6. Argument 3: Combinative effect – mistakes by judges.....	243
3.6.1 Consent and necessity.....	244
3.6.2 ‘Right to immediate possession’ in the context of a blockchain token.....	246
3.6.3 Frozen token.....	249
3.6.4 ‘Digital trespass and conversion’ cases in other jurisdictions.....	254
4. Option 2: A new regime.....	257
4.1 Impairment tort.....	258
4.1.1 The conduct element.....	258
4.1.2 The mental element.....	264
4.1.2.1 A lower threshold? .....	266
4.1.3 Superior and inferior property rights.....	268
4.2 ‘Recovery of control’ remedy.....	269
4.3 How this regime is superior to extending the chattel torts to digital assets.....	271
4.3.1 ‘Recovery of control’ remedy.....	271
4.3.2 Impairment tort.....	273
4.3.2.1 ‘Prima facie’ liability: the conduct and mental elements.....	273
4.3.2.2 Defences.....	275
4.4 Why legislation is better than case law development.....	276
5. Conclusion.....	277
 <b>Conclusion and Future Directions.....</b>	 278
1. Summary of arguments.....	278
2. Further research directions.....	280
 Bibliography.....	 282

## Table of Abbreviations

- AML – Anti-money laundering
- API – Application programming interface
- DAL – Dubai International Financial Centre, Digital Assets Law (DIFC Law No. 2 of 2024)
- DAO – Decentralised autonomous organisation
- DDoS – Distributed denial of service
- DeFi – Decentralised finance
- DLT – Distributed ledger technology
- DIFC – Dubai International Financial Centre
- ETF – Exchange-traded fund
- EUA – EU allowance
- FCARs – Financial Collateral Arrangements (No 2) Regulations 2003 (SI 2003/3226)
- FCD – Directive 2002/47/EC of the European Parliament and of the Council of 6 June 2002 on financial collateral arrangements
- ICO – Initial coin offering
- IDS – Intrusion detection system
- KYC – Know your customer
- LRA – Land Registration Act 2002
- Multisig – Multi-signature
- NFT – Non-fungible token
- SGA – Sale of Goods Act 1979

## Table of Cases

<i>AA v Persons Unknown</i> [2019] EWHC 3556 (Comm) .....	40-43, 46
<i>AB v Leeds Teaching Hospital NHS Trust</i> [2004] EWHC 644 (QB).....	72
<i>Agnew v Commissioners of Inland Revenue</i> [2001] UKPC 28.....	141
<i>Akers v Samba Financial Group</i> [2017] UKSC 6, [2017] AC 424.....	253
<i>Ancona v Rogers</i> (1876) 1 Ex D 285 .....	111
<i>Armstrong v Winnington</i> [2012] EWHC 10 (Ch), [2013] Ch 156 .....	55
<i>Barclays Bank v Various Claimants</i> [2020] UKSC 13, [2020] AC 973 .....	140
<i>Berezovsky v Abramovich</i> [2011] EWCA Civ 153, [2011] 1 WLR 2290 .....	208
<i>Bolam v Friern Hospital Management Committee</i> [1957] 1 WLR 582.....	118
<i>Borden (UK) Ltd v Scottish Timber Products Ltd</i> [1981] Ch 25.....	148
<i>Borwick Development v Clear Water Fisheries</i> [2020] EWCA Civ 578, [2021] Ch 153.....	135
<i>Bristol Airport Plc v Powdrill</i> [1990] Ch 744, [1990] BCC 130.....	31, 126
<i>Burroughes v Bayne</i> (1860) 5 H & N 296.....	58, 219, 222, 249-252
<i>Campbell v Mirror Group Newspapers</i> [2004] UKHL 22, 2 AC 457.....	209
<i>CC Kent Police v Taylor</i> [2022] EWHC 737.....	209
<i>Re Celtic Extraction Ltd</i> [2001] Ch 475.....	63
<i>Clayton v Roy</i> [1911] 2 KB 1031.....	219
<i>Club Cruise Entertainment v Department of Transport</i> [2008] EWHC 2794 (Comm), [2009] 1 All ER (Comm) 955 .....	220, 251-252
<i>Cochrane v Moore</i> (1890) 25 QBD 57.....	161, 163-164
<i>Colonial Bank v Whinney</i> [1885] 30 Ch D 261.....	11, 41, 46
<i>Costello v Chief Constable of Derbyshire Constabulary</i> [2001] EWCA Civ 381, [2001] 1 WLR 1437.....	96, 116
<i>Crantrave Ltd v Lloyds Bank plc</i> [2000] EWCA Civ 127, [2000] QB 917.....	63
<i>Collins v Wilcock</i> [1984] 1 WLR 1172.....	220
<i>Cope v Sharpe (No 2)</i> [1912] 1 KB 496.....	233
<i>Dearle v Hall</i> (1828) 3 Russ 1.....	112

<i>De Mattos v Gibson</i> (1859) 45 ER 108.....	125, 127
<i>Dobson v North Tyneside Health Authority</i> [1996] 4 All ER 474.....	72
<i>Donoghue v Stevenson</i> [1932] AC 562.....	268
<i>Earl of Worcester v Finch</i> (1600) 2 And 162.....	253
<i>England v Cowley</i> (1873) LR 8 Exch 126.....	219
<i>Fetch.ai v Persons Unknown</i> [2021] EWHC 2254 (Comm) .....	44
<i>Gordon v Harper</i> (1796) 7 TR 9, 101 ER 828.....	121, 123-125
<i>Government of the Islamic Republic of Iran v Barakat Galleries Ltd</i> [2007] EWCA Civ 1374, [2009] QB 22.....	133, 247
<i>Gray v G-T-P Group Ltd</i> [2010] EWHC 1772 (Ch).....	141
<i>Ion Science v Persons Unknown</i> (unreported), 21 December 2020 (Commercial Court).....	44
<i>Halliday v Holgate</i> (1868) LR 3 Ex 299.....	123
<i>Hedley Byrne &amp; Co Ltd v Heller &amp; Partners Ltd</i> [1963] UKHL 4, [1964] AC 465.....	210
<i>Hill v Tupper</i> (1863) 2 H & C 121, 159 ER 51.....	102
<i>Hollins v Fowler</i> (1872) LR 7 HL 757.....	239
<i>HSBC Rail (UK) Ltd v Network Rail Infrastructure Ltd</i> [2005] EWCA Civ 1437, [2006] 1 WLR 643.....	182
<i>Investec Trust (Guernsey) Ltd v Glenalla Properties Ltd</i> [2018] UKPC 7, [2019] AC 271.....	253
<i>J A Pye (Oxford) Ltd v Graham</i> [2002] UKHL 30, [2003] 1 AC 419.....	110, 141, 241
<i>Jarvis v Williams</i> [1955] 1 WLR 71.....	133, 247
<i>Jeffries v Great Western Railway Co</i> (1856) 5 E&B 802, 119 ER 680.....	116
<i>Jones v First-Tier Tribunal</i> [2013] UKSC 19, [2013] 2 AC 48.....	129
<i>Keppell v Bailey</i> (1834) 2 My & K 517, 47 ER 106.....	102
<i>Kirk v Gregory</i> (1876) 1 Ex D 55.....	233
<i>Re Lehman Brothers International (Europe) (In Administration)</i> [2012] EWHC 2997 (Ch).....	141
<i>Lancashire and Yorkshire Railway Co v MacNicoll</i> (1918) 88 LJKB 601.....	239
<i>Leigh &amp; Sullivan Ltd v Aliakmon Shipping Co Ltd (The Aliakmon)</i> [1986] AC 785.....	252-253

<i>Lord Compton's Case</i> (1580) 3 Leo 197.....	253
<i>Lumley v Gye</i> (1853) 2 E&B 216.....	127, 133
<i>Mainline Private Hire Ltd v Nolan</i> [2011] EWCA Civ 189.....	93, 95
<i>Manchester Airport Plc v Dutton</i> [1999] EWCA Civ 844, [2000] QB 133.....	247-249
<i>Maynard v West Midlands RHA</i> [1984] 1 WLR 634.....	118
<i>MCC Proceeds v Lehman Brothers International (Europe)</i> [1997] EWCA Civ 3068, [1998] 4 All ER 676.....	133, 253
<i>Monsanto plc v Tilly</i> [1999] EWCA Civ 3044, [2000] Env LR 313.....	233
<i>Montgomery v Lanarkshire Health Board</i> [2015] UKSC 11, [2015] 1 AC 1430.....	118
<i>Murphy v Brentwood DC</i> [1991] UKHL 2, [1991] 1 AC 398.....	209
<i>National Provincial Bank v Ainsworth</i> [1965] UKHL 1 [1965] AC 1175.....	30-31, 41-51, 126
<i>Newcastle-under-Lyme Corp v Wolstanton Ltd</i> [1947] Ch 92.....	70
<i>OBG Ltd v Allan</i> [2007] UKHL 21, [2008] 1 AC 1.....	63, 108, 113, 114, 115, 127, 134, 142, 207, 208, 241, 247, 248, 253, 255
<i>Osbourne v Persons Unknown</i> [2022] EWHC 1021.....	44
<i>Official Assignee of Madras v Mercantile Bank of India</i> [1935] AC 53.....	112
<i>Parker v British Airways Board</i> [1982] 1 QB 1004.....	105, 107
<i>The Pioneer Container</i> [1994] 2 AC 324.....	118-121
<i>Port Line Ltd v Ben Line Steamers Ltd</i> [1958] 2 QB 146.....	127
<i>Powell v McFarlane</i> (1977) 38 P & CR 452.....	87, 110, 141, 241
<i>Prince Jefri Bolkiah v KPMG</i> [1998] UKHL 52, [1999] 2 AC 222.....	209
<i>Private Equity Insurance Group SIA v Swedbank AS</i> (C-156/15) [2017] EU:C:2016:851, 1 WLR 1602, [2017] 1 BCLC 207.....	141, 198-199
<i>R (Privacy International) v Investigatory Powers Tribunal</i> [2019] UKSC 22, [2020] 2 AC 491.....	129
<i>R v G</i> [2003] UKHL 50, [2004] 1 AC 1034.....	265
<i>R v Kelly</i> [1998] EWCA Crim 1578, [1999] QB 621.....	72

<i>R v Sharpe</i> (1857) Dears & B 160.....	72
<i>Richardson v Atkinson</i> (1723) 1 Stra 576; 93 ER 710.....	219
<i>Read v Lyons &amp; Co Ltd</i> [1945] KB 216.....	70
<i>Sanders Bros v Maclean &amp; Co</i> (1883) 11 QBD 327.....	111
<i>Secretary of State for Health v Servier Laboratories Ltd</i> [2019] EWCA Civ 1160, [2020] Ch 717.....	208
<i>Shell UK Ltd v Total UK Ltd</i> [2010] EWCA Civ 180, [2011] QB 86.....	134, 248, 252-253
<i>Smith v Eric S Bush</i> [1990] UKHL 1, [1990] 1 AC 831.....	210
<i>Sorrell v Paget</i> [1950] 1 KB 252.....	233
<i>Re Spectrum Plus</i> [2005] UKHL 41, [2005] 2 AC 880.....	141
<i>Spring v Guardian Assurance plc</i> [1994] UKHL 7, [1995] 2 AC 296.....	210
<i>Standing v Bowring</i> (1885) 31 Ch D 282.....	172
<i>Transco Plc v United Water Utilities Plc</i> [2005] EWHC 2784 (QB) .....	263
<i>Tchenguiz v Imerman</i> [2010] EWCA Civ 908, [2011] 2 WLR 592.....	209
<i>Thomas v Times Book Co Ltd</i> [1966] 2 All ER 241.....	163
<i>Watts v Stewart</i> [2016] EWCA Civ 1247, [2017] 2 WLR 1107.....	112
<i>Westdeutsche Landesbank Girozentrale v Islington London</i> <i>Borough Council</i> [1996] UKHL 12, [1996] 1 AC 669.....	49, 207, 270, 272
<i>White v Jones</i> [1995] UKHL 5, [1995] 2 AC 207.....	210
<i>William Leitch and Co Ltd v Leydon</i> [1931] AC 90.....	263
<i>Williams v Williams</i> [1882] 20 Ch D 659.....	72
<i>Willis v British Car Auctions</i> [1978] 1 WLR 438.....	241
<i>Wilson v Lombank</i> (1963) 1 WLR 1294.....	111
<i>The Winkfield</i> [1902] P 42.....	125
<i>Yearworth v North Bristol NHS Trust</i> [2009] EWCA Civ 37, [2010] QB 1.....	29, 72, 118-119
<i>Your Response v Datateam</i> [2014] EWCA Civ 281, [2015] QB 41.....	108, 113-115, 143

## **Australia**

<i>Bunnings Group Ltd v CHEP Australia Ltd</i> [2011] NSWCA 342.....	239-240
--	---------

<i>Chairman, National Crime Authority v Flack</i> [1998] FCA 932; (1998) 86 FCR 16.....	107
<i>Doodeward v Spence</i> (1908) 6 CLR 406.....	72
<i>Hutchins v Maughan</i> [1947] VLR 131.....	222
<i>Mallonland Pty Ltd v Advanta Seeds Pty Ltd</i> [2024] HCA 25.....	268

## **Canada**

<i>Canivate Growing Systems Ltd v Brazier</i> [2020] BCSC 232.....	215
--	-----

## **Hong Kong**

<i>Re Gatecoin Ltd</i> [2023] HKCFI 914.....	47
--	----

## **New Zealand**

<i>Henderson v Walker</i> [2019] NZHC 2184.....	215
<i>Ruscoe v Cryptopia Ltd</i> [2020] NZHC 728.....	44-47

## **Singapore**

<i>B2C2 v Quoine</i> [2019] SGHC(I) 3.....	42, 47, 49
<i>ByBit Fintech Limited v Ho Kai Xin</i> [2023] SGHC 199.....	49, 50, 63, 77, 207, 270
<i>CLM v CLN and Others</i> [2022] SGHC 46.....	44
<i>The Endurance I</i> [2000] SGHC 99.....	239
<i>Janesh s/o Rajkumar v Unknown Person</i> [2022] SGHC 264.....	44
<i>Quoine v B2C2</i> [2020] SGCA(I) 2.....	47, 49
<i>Simgood Pte Ltd v MLC Shipbuilding Sdn Bhd</i> [2015] SGHC 303.....	133

## **United States**

<i>Archer v Coinbase Inc</i> 53 Cal App 5th 266, 267 Cal Rptr 3d 510 (Cal Ct App 2020) .....	255
<i>CompuServe v Cyber Promotions</i> 962 F. Supp 1015 (SD Ohio 1997).....	215, 254
<i>Kleiman v Wright</i> Case No. 18-CV-80176-BLOOM/Reinhart (SD Fla Dec 27, 2018) .....	255
<i>Kremen v Cohen</i> 337 F.3d 1024 (9th Cir, 2003) .....	215

*Shin v ICON Foundation* (Case No. 20-cv-07363-WHO (ND Cal May 11, 2021)).....250, 255-256

*Williams v Mahmood* (Case No. 6:21-cv-03074-RK) .....255

## Table of Statutes

### United Kingdom

Cheques Act 1957.....	223
s.4.....	223
Criminal Damage Act 1971.....	76, 265
s.1.....	76, 265
s. 1(1) and 1(2) .....	265
Electronic Trade Documents Act 2023.....	207
s.3.....	207
Employment Relations Act 1999.....	140
Employment Rights Act 1996.....	140
Equality Act 2010.....	140
Factors Act 1889.....	112, 165
s.2(1) .....	165
s.3.....	112
Insolvency Act 1986.....	31, 126, 223
s.234(3) .....	223
s.307(4) .....	223
s.346(7) .....	223
s.436.....	31, 126
Land Registration Act 2002.....	195
s.58.....	195
Law of Property Act 1925.....	248
s.1.....	248
Law of Property (Miscellaneous Provisions) Act 1989.....	161
s.1(2) .....	161
s.1(3) .....	161

Limitation Act 1980.....	98-99
s.2.....	99
s.3.....	98, 99
s.4.....	98
s.15.....	98
s.17.....	98
Misuse of Drugs Act 1971.....	112-113
s.5.....	112
s.28.....	113
s.37(3) .....	113
National Minimum Wage Act 1998.....	140
Sale of Goods Act 1979.....	164-166
s.2(1) .....	164-165
s.17.....	164-166
ss.21-25.....	165
Theft Act 1968.....	76
s.1(1) .....	76
Torts (Interference with Goods) Act 1977.....	223, 271-272
s.3.....	271-272
s.8(1) .....	223

## **New Zealand**

Companies Act 1993.....	44
s.2.....	44

## **Hong Kong**

Companies (Winding Up and Miscellaneous Provisions) Ordinance (Cap. 32) .....	47
---	----

s.197.....	47
Interpretation and General Clauses Ordinance (Cap. 1) .....	47
s.3.....	47

## European Union

Directive 2002/47/EC of the European Parliament and of the Council of 6 June 2002 on financial collateral arrangements. ....	146
--	-----

## Dubai International Financial Centre

Dubai International Financial Centre, Digital Assets Law (DIFC Law No. 2 of 2024).....	17, 18, 34, 53, 58-62, 69, 93, 105, 150-151, 168, 177, 184, 188-189, 211, 263, 266, 269-270
Article 8.....	17, 53
Article 9.....	17
Article 10.....	17, 93, 177, 184, 189, 190
10(1) .....	93, 189
10(1)(a) .....	189
10(3) .....	93, 177, 189, 190
10(3)(a) .....	93, 189
10(3)(b) .....	184, 189, 190
Article 11.....	17, 93, 105
11(1) .....	105
Article 12.....	17, 34, 61, 150, 168, 177, 184, 188
12(1) .....	34, 61, 150, 184
Article 13.....	17
Article 14.....	17, 58-60, 62, 69, 151, 211, 263, 266, 269

14(1) .....	59, 62, 69, 211, 266, 269
14(1)(b) .....	62, 69
14(1)(c) .....	62, 69
14(1)(c)(i) .....	59
14(2) .....	58, 60, 62, 211, 263, 266
14(2)(b) .....	60, 263
14(2)(c) .....	58, 62, 211, 266
14(2)(d) .....	58, 60
Article 15.....	17, 270
15(1)(a) .....	270
15(1)(b) .....	270

## Table of Other Primary Legal Sources

### United Kingdom

Financial Collateral Arrangements (No 2) Regulations 2003 (SI 2003/3226).....	139-141, 145-147
Reg 3.....	139, 141
Parts 2, 3 and 4.....	141
Property (Digital Assets etc) HL Bill (2024-25) .....	11, 17

## **Introduction**

This thesis discusses the legal nature of digital assets, from a property law perspective. It explores the following research questions:

1. Whether digital assets are conceptually capable of being the subject-matter of property rights, and if so, whether it is normatively desirable to recognise a property right in digital assets; and
2. The circumstances in which it should be possible to acquire a property right in a digital asset for the first time; and
3. The circumstances in which it should be possible to transfer a property right in a digital asset; and
4. The nature and extent of protection against third parties generally that ought to be offered to a holder of a property right in a digital asset.<sup>1</sup>

### **1. Background**

Digital assets constitute a three trillion dollar asset class,<sup>2</sup> and with such significant amounts of money being invested into digital assets, it is crucial to have legal rules that determine people's rights and obligations in relation to digital assets, including from a property law perspective.

Yet, there is relatively little legal clarity about the private law rules that govern digital assets, including in relation to my four research questions. This is largely because digital assets

---

<sup>1</sup> I will refer to these as my first, second, third, and fourth research questions respectively.

<sup>2</sup> The market capitalisation for cryptoassets is 3.17 billion USD as of 31<sup>st</sup> December 2024: 'Cryptocurrency Prices, Charts And Market Capitalizations | CoinMarketCap', *CoinMarketCap* at <https://coinmarketcap.com> (accessed 31 December 2024).

remain a relatively new asset class, which has only entered the mainstream approximately eight years ago during the 2017-18 initial coin offering (ICO) boom.

In order to understand the rise of digital assets, it would be helpful to start from the aftermath of the 2008 financial crisis. During that time, movements like Occupy Wall Street characterised the sentiment that many felt towards banks and centralised financial entities, namely a feeling of deep distrust and suspicion towards them. The financial crisis made people realise that banks were not in fact as safe as they previously thought, and could be quite fragile given the interconnectedness of the financial system.

Many people wanted a decentralised way of storing and moving value, and the pseudonymous ‘Satoshi Nakamoto’ creating Bitcoin in 2009.<sup>3</sup> He created Bitcoin because he wanted a system by which value could be moved without the cooperation of a central intermediary.<sup>4</sup> He successfully created such a system by launching the Bitcoin network.

Bitcoin is the first cryptocurrency in the world, and its invention produced an unprecedented breakthrough. The breakthrough of Bitcoin was its solution to the ‘double spending’ problem (the problem of not having any reliable way to prevent a person from spending the same money twice)<sup>5</sup> without the need for a trusted intermediary. This was achieved through the combination of cryptographic technology, software, a distributed ledger, and the provision of a set of incentives for people to maintain the operation of the system.

In previous forms of digital currency, the double spending problem was addressed by the use of a central intermediary.<sup>6</sup> This did not create sufficient economic disincentives against

---

<sup>3</sup> The Bitcoin network was launched on 3 January 2009 (see Joshua Davis, 'The Crypto-Currency | The New Yorker', *The New Yorker*, <http://www.newyorker.com/magazine/2011/10/10/the-crypto-currency> (accessed 29 December 2024)), but Satoshi Nakamoto wrote the Bitcoin White Paper in 2008 (Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008) (at <https://bitcoin.org/bitcoin.pdf>, accessed 31 December 2024).

<sup>4</sup> Nakamoto (n 3 above), 1.

<sup>5</sup> See e.g. 'Double spend (problem) – Glossary | CSRC', *CSRC* at [https://csrc.nist.gov/glossary/term/double\\_spend\\_problem](https://csrc.nist.gov/glossary/term/double_spend_problem) (accessed 31 December 2024).

<sup>6</sup> Jamie Redman, 'Before Bitcoin: 4 Early Digital Currencies and Why They Collapsed – Learning – Insights Bitcoin News', *Bitcoin News* at <https://news.bitcoin.com/before-bitcoin-4-early-digital-currencies-and-why-they-collapsed/> (accessed 29<sup>th</sup> December 2024).

unilateral tampering, because the operator of the master ledger that recorded all the account balances could unilaterally modify the entries containing the balances, by manually changing the entries on (e.g.) the relevant Excel file or other database record. He could simply do so to benefit himself – e.g. by increasing the balance of such currency in his account. Unsurprisingly, digital currencies prior to Bitcoin did not gain mass adoption.<sup>7</sup>

In the context of Bitcoin, this problem of unilateral tampering does not arise because of several features it contains. First, the Bitcoin ledger is a distributed ledger, meaning that multiple computers (‘nodes’) have the same copies of the same ledger. Second, in order to modify the Bitcoin ledger, one must satisfy Bitcoin’s consensus rules (‘consensus algorithm’) that determine when a proposed entry on the ledger is valid. Its consensus algorithm is based on ‘proof of work’, where the person who demonstrates that he has solved a computationally difficult mathematical puzzle (the ‘miner’) is able to add groups of entries onto the ledger provided that other nodes<sup>8</sup> on the network have verified the transaction(s). Third, miners who manage to solve the puzzle are rewarded in Bitcoin, which provides the economic incentive for them to maintain the network and keep running nodes on the Bitcoin network. Fourth, it is easy to detect whether a proposed block contains an existing ledger entry that has been fraudulently modified, because the use of what are known as ‘cryptographic hash functions’. Cryptographic hash functions are mathematical functions that convert any raw data into a fixed alphanumeric string<sup>9</sup> (the ‘hash’), where a change in the raw data (no matter how small) creates a wildly different alphanumeric string.

---

<sup>7</sup> See e.g. *ibid*; other examples of digital currencies that failed to gain mass adoption include Flooz and Beenz, DIGicash, Mondex, and Cybercash.

<sup>8</sup> The majority of full nodes. Nodes are participants in the Bitcoin network, and full nodes are participants that maintain complete copies of the blockchain and validate transactions according to the protocol rules.

<sup>9</sup> See also e.g. Howard Poston, 'Hash Functions in Blockchain', *Infosec* at <https://www.infosecinstitute.com/resources/blockchain-security-overview/hash-functions-in-blockchain/> (accessed 31<sup>st</sup> December 2024).

Thus, in the case of Bitcoin, if a person wants to fraudulently modify the ledger, he would have to prove that he has solved the relevant mathematical puzzle, which costs a lot of computational power and is (and has been for a long time) much more costly than the Bitcoin rewards conferred on miners to successfully solve the computational puzzle. This means it is uneconomical to attempt such a fraud – hence it is said that Bitcoin is ‘tamper proof’.<sup>10</sup>

This general technology that underpins the Bitcoin system underpins other cryptoassets as well, though there can be different consensus algorithms such as Proof of Stake, Delegated Proof of Stake, Proof of History, and Proof of Authority.<sup>11</sup> This general technology is called blockchain technology, and assets on a blockchain have been described as ‘digital assets’.

Since 2009, there have been many developments in the digital asset space that have attracted the interest of developers, blockchain<sup>12</sup> users and enthusiasts, as well as retail and institutional investors.

For example, the Ethereum blockchain and ecosystem allowed for the creation of smart contracts on the blockchain. A smart contract is, in essence, programmable code that is stored on the blockchain, and is executed when specified conditions are met.<sup>13</sup> This is extremely useful in the context of (e.g.) escrow and succession arrangements where conditions need to be satisfied before assets on the blockchain are released, and parties do not want to rely on a centralised third party source. The code itself (and the underlying blockchain technology) provides the necessary security for parties, and parties can tailor the conditions under which

---

<sup>10</sup> Nonetheless, Bitcoin can be subject to what are known as 51% attacks (where a single entity gains control of over 50% of the mining power, allowing them to manipulate transactions and double-spend coins). This is theoretically possible, but it is practically infeasible due to the immense cost of acquiring the necessary mining power, the decentralized nature of the network, and the significant financial risks associated with damaging trust in the system. The economic incentives for miners to act honestly further deter such attacks, making them unlikely in reality.

<sup>11</sup> The precise consensus algorithm adopted depends on the design of the blockchain or distributed ledger, and is chosen based on factors such as security, scalability, decentralisation, and energy efficiency.

<sup>12</sup> See Chapter 1, Section 2 (text to nn 2-3) below for the meaning of a blockchain.

<sup>13</sup> The code is self-executing: see e.g. smart contracts on the Ethereum blockchain.

the relevant funds are to be released. With smart contract arrangements, there is a lot of flexibility to compose the arrangement that one wants.

The Ethereum blockchain has also provided the foundation for further developments such as non-fungible tokens (NFTs), Layer 2 technology,<sup>14</sup> the tokenisation of assets<sup>15</sup> and an increasing variety of smart contracts. It has also fuelled the creation and development of other blockchains that do the same, such as Solana. Furthermore, blockchain technology has been used for electronic trade documents – for example CargoX uses the Ethereum blockchain to issue tokens (which are the electronic trade documents) and store data<sup>16</sup> about the underlying paper documents that are uploaded onto the relevant platform.<sup>17</sup>

Over the last four years, there have been increasing amounts of institutional interest and engagement in the digital asset space. More investments are being made in the digital asset space,<sup>18</sup> and there are now many regulated investment products in respect of digital assets, including many exchange-traded funds (ETFs) in relation to Bitcoin and Ether.<sup>19</sup> It is anticipated that there may be ETFs in respect of Solana as well.<sup>20</sup>

---

<sup>14</sup> E.g. enhanced scalability (more transactions per second) while leveraging the security guarantees of the underlying Layer 1 blockchain.

<sup>15</sup> Tokenisation is the process of creating a digital asset that represents rights to a separate asset (such as a bond, share, or physical asset).

<sup>16</sup> Specifically the hash.

<sup>17</sup> Issuing an electronic bill of lading under the CargoX system involves minting a non-fungible token on the Ethereum blockchain that contains the hash of the relevant paper document(s) uploaded on the Interplanetary File System (IPFS). This token is the electronic trade document. See Vjeran Ortynski and Janez Kranjc, 'Blockchain document transfer: understanding the technology and its uses', *CargoX* at <https://cargox.io/content-hub/blockchain-document-transfer-understanding-technology-and-its-uses> (accessed 10th September 2024), and Patrick Vlacic and Bojan Cekrljic, 'The legality of an electronic bill of lading | CargoX', *CargoX* at <https://cargox.io/content-hub/legal-ity-electronic-bill-lading> (accessed 10th September 2024). Wave BL and edoxOnline also use the Ethereum blockchain for their e-bills of lading (eBOL) services.

<sup>18</sup> See e.g. 'Institutional Money Is Flowing Back Into Crypto – Here's How Margex Copy Trading Helps You to Approach the Markets', *CryptoSlate* at <https://cryptoslate.com/institutional-money-is-flowing-back-into-crypto-heres-how-margex-copy-trading-helps-you-to-approach-the-markets/> (accessed 10th September 2024) (\$17 billion of institutional capital flowing into the cryptocurrency space).

<sup>19</sup> For example, as of 10<sup>th</sup> September 2024, there are 31 Bitcoin ETFs and 10 Ether ETFs that are listed in the US (see e.g. 'Bitcoin ETF List', *Vettafi* at <https://etfdb.com/themes/bitcoin-etfs/> (accessed 10<sup>th</sup> September 2024) and 'Ethereum ETF List', *Vettafi* at <https://etfdb.com/themes/ethereum-etfs/> (accessed 10<sup>th</sup> September 2024)), six Bitcoin/Ether ETFs in Hong Kong (see e.g. 'Asia's First Spot Bitcoin and Ether ETFs Debut in Hong Kong', *Hauzen* at <https://hauzen.hk/asias-first-spot-bitcoin-and-ether-etfs-debut-in-hong-kong> (accessed 10th September 2024)).

<sup>20</sup> Institutions have also filed applications for Solana ETFs, such as 21Shares (see e.g. Derek Andersen, '21Shares files application application for spot Solana ETF', *Cointelegraph* at

Opinions are very divided about digital assets. On the one hand, there are people who are very optimistic and bullish about the digital asset space and how it can significantly enhance or revolutionise various industries. On the other hand, there are people who are extremely critical of digital assets and believe that they are very harmful to society or at least of limited utility.

Many people believe that there are various valuable use cases of digital assets, for example in the context of (e.g.) smart contracts, decentralised finance (DeFi), non-fungible tokens (NFTs), and decentralised autonomous organisations (DAOs).<sup>21</sup> These have the potential to materially enhance the fields of (*inter alia*) finance, art, and collective decision-making.<sup>22</sup>

For example, the advent of DAOs has given rise to an increased range of mechanisms to make collective decisions and distribute power within an organisation or community.<sup>23</sup> DeFi has led to a wider range of automated and more efficient financial services,<sup>24</sup> and has the

---

<https://cointelegraph.com/news/21shares-spot-solana-etf-sec> (accessed 10th September 2024)) and VanEck (see e.g. Frances Yue, 'Why VanEck's solana ETF application is a win for crypto – even if it's not approved | Morningstar', *Morningstar* at <https://www.morningstar.com/news/marketwatch/20240627378/why-vanecks-solana-etf-application-is-a-win-for-crypto-even-if-its-not-approved> (accessed 10th September 2024)).

<sup>21</sup> A DAO is a governance structure where tokenholders can vote and make decisions in relation to an entity, community, or organisation, according to its rules. Power resides with the tokenholders instead of a central authority. See e.g. Nathan Reiff, 'Decentralized Autonomous Organization (DAO): Definition, Purpose, and Example', *Investopedia* at <https://www.investopedia.com/tech/what-dao/#:~:text=A%20decentralized%20autonomous%20organization%20is,holders%20who%20collectively%20cast%20votes> (accessed 1<sup>st</sup> January 2025).

<sup>22</sup> See e.g. Benjamin Quinlan and David Wills, 'A New Chain of Thought: Exploring the Building Blocks of the Next Digital Era' (Quinlan and Associates, 2024); Benjamin Quinlan, Justin Chung and Eashan Trehan, 'Cracking the Code: The Evolution of Digital Assets to the Mainstream' (Quinlan and Associates, 2021); Benedicte N. Nolens and Benjamin Quinlan, 'Project Dynamo: CBDCs, Stablecoins, and Deposit Tokens: Wholesale Adoption Explorations and Challenges' (BIS Innovation Hub and Quinlan and Associates, 2023).

<sup>23</sup> See e.g. Decentraland, MolochDAO, MakerDAO, and Compound. See also 'Four Industries Where DAOs Thrive: Key Use Cases Explored', *Colony* at <https://blog.colony.io/what-are-dao-real-world-use-cases/> (accessed 12<sup>th</sup> September 2024), and Law Commission of England and Wales, *Decentralised Autonomous Organisations (DAOs) – A scoping paper* (2024), chapter 2.

<sup>24</sup> See e.g. Uniswap, SushiSwap, Aave, Compound, and MakerDAO. These services include a much-reduced level of human onboarding and involvement (as compared to traditional financial services), as users can (e.g.) obtain loans and trade assets in an automated, quick, decentralised, and customisable manner. See also 'Blockchain for Decentralised Finance (DeFi) | Consensys', *Consensys* at <https://consensys.io/blockchain-use-cases/decentralized-finance> (accessed 12th September 2024).

potential to significantly enhance existing financial services.<sup>25</sup> In turn, the use of NFTs has led to increased opportunities for creatives (such as artists and musicians), and business owners, to engage with their community and diversify their revenue streams.<sup>26</sup> Smart contracts, which are crucial to the use cases mentioned, can also be used for the transfer and safekeeping of assets under escrow and custodial arrangements (e.g. in the institutional business context and the succession context).<sup>27</sup>

On the other hand, many people also believe that digital assets (or certain types of digital assets) are harmful to society and of very limited utility. One of the most vocal critics of cryptoassets in legal academia is Robert Stevens, who contends that “Bitcoins...are of even less inherent utility than the children’s daubs in [his] loft”,<sup>28</sup> and that “[cryptoassets are] the largest pyramid scheme ever yet dreamed up”.<sup>29</sup> He also believes that cryptoassets are a “solution to a commercial need that does not exist”, and that “nobody has, as yet, has discovered a commercially important legal use for it”.<sup>30</sup> Furthermore, he notes the negative environmental implications of cryptoassets as well as the benefits that cryptoassets bring in relation to criminals.<sup>31</sup>

---

<sup>25</sup> See e.g. Andry Alamsyah, Gede Natha Wijaya Kusuma and Dian Puteri Ramadhani, ‘A Review on Decentralised Finance Ecosystems’ (2024) 16 *Future Internet* 76; see also Tyler Cowen and Alex Tabarrok, ‘Cryptoeconomics’ at <https://marginalrevolution.com/wp-content/uploads/2022/05/Cryptoeconomics-Modern-Principles.pdf> (accessed 12<sup>th</sup> September 2024), 18-19 (lending opportunities for poorer individuals).

<sup>26</sup> See e.g. Cryptopedia Staff, ‘NFT Art and Music: Blockchain Music Use Cases’, *Gemini* at <https://www.gemini.com/cryptopedia/nft-crypto-blockchain-music-industry> (accessed 12<sup>th</sup> September 2024) (increased profits and royalties for artists; not needing to give up a large proportion of profits to labels and streaming platforms); Anatoli Colicev, ‘How can non-fungible tokens bring value to brands’ (2023) 40(1) *Int J Res Mark* 30 (increased engagement with community via e.g. exclusive Discord servers).

<sup>27</sup> See e.g. Safe (formerly Gnosis Safe), and Unchained. Also, on the international front, the International Swaps and Derivatives Association recognises the applicability of smart contract technology in automating and implementing payment obligations under FX confirmations: see International Swaps and Derivatives Association, ‘ISDA Legal Guidelines for Smart Derivatives Contracts: Foreign Exchange Derivatives’ (2020), 13-14.

<sup>28</sup> Robert Stevens, ‘Crypto is not property’ (2023) 139 *LQR* 615, 620.

<sup>29</sup> *ibid*, 621.

<sup>30</sup> *ibid*, 627.

<sup>31</sup> *ibid*, 627.

Indeed, many digital assets have been the subject of hacks and bugs. Well-known examples include the DAO hack (where around \$60m worth of Ether was drained),<sup>32</sup> the Wormhole bridge hack (where more than \$320m worth of crypto was drained),<sup>33</sup> and the Ronin hack (where more than \$600m worth of crypto was drained).<sup>34</sup> There are many possible hacks and attacks, such as 51% attacks,<sup>35</sup> smart contract exploits,<sup>36</sup> and distributed denial of service (DDoS) attacks.<sup>37</sup> Lots of digital assets can be misappropriated or denied access to, and as digital assets have high valuations, hacks and attacks can cause vast amounts of monetary loss. The stakes are immense.

But what is undeniable is that in the digital asset space, there is an enormous amount of money flowing around as many digital assets are being bought, sold and transferred on a daily basis.<sup>38</sup> This consists of lot of ‘illegal money’ but also a lot of legal money (in the retail and institutional contexts).

As mentioned however, there is a relative lack of clarity about the legal aspects of digital assets, including from a property law perspective. For example, when someone denies access to a digital asset that is in your control, or disables the functionalities that you can exercise in respect of such a digital asset, what remedies do you have? Also, what are the requirements that need to be satisfied for you to sell a digital asset – do you (for example) need

---

<sup>32</sup> David Z. Morris, 'CoinDesk Turns 10: 2016 - How The DAO Hack Changed Ethereum and Crypto', *CoinDesk* at <https://www.coindesk.com/consensus-magazine/2023/05/09/coindesk-turns-10-how-the-dao-hack-changed-ethereum-and-crypto> (accessed 31 December 2024); Cryptopedia Staff, 'The DAO: What Was the DAO Hack? | Gemini', *Gemini* at <https://www.gemini.com/cryptopedia/the-dao-hack-makerdao> (accessed 31<sup>st</sup> December 2024).

<sup>33</sup> Brian Newar, 'Wormhole Token Bridge Loses \$321M in Largest Hack So Far in 2022', *Cointelegraph* at <https://cointelegraph.com/news/wormhole-token-bridge-loses-321m-in-largest-hack-so-far-in-2022> (accessed 31<sup>st</sup> December 2024).

<sup>34</sup> yycrader, 'Axie Infinity's Ronin Bridge Exploited For More Than \$600M – “The Defiant”', *The Defiant* at <https://thedefiant.io/news/nfts-and-web3/axie-infinity-hack-600m> (accessed 31<sup>st</sup> December 2024).

<sup>35</sup> Where a single entity gains control of over 50% of the computational power or staking power, allowing them to manipulate transactions and double-spend coins.

<sup>36</sup> Which can drain a smart contract address of all its assets.

<sup>37</sup> I.e. when numerous computers send an overwhelming amount of traffic to a website or online service, causing it to slow down or become unavailable.

<sup>38</sup> See e.g. 'Live Cryptocurrency Charts & Market Data | Coinmarketcap', *Coinmarketcap* at <https://coinmarketcap.com/charts/> (accessed 26<sup>th</sup> December 2024) – daily trading volume of 117.79 billion USD as of 26<sup>th</sup> December 2024.

to execute an on-chain transfer, change control of the asset, or would an oral agreement be sufficient? And how does one acquire an original property right to a digital asset for the first time? More fundamentally, are digital assets even capable of being the subject-matter of a property right?

These questions matter in many contexts, for example when a person who has been deprived of control of a digital asset or is disabled from exercising functionalities in respect of the digital asset seeks to sue for damages or (in the former case) for recovery of the digital asset. We need to know what remedies he is entitled to and (often) whether there is a legal wrong (breach of duty),<sup>39</sup> which depends on whether he has a property right to the asset, which in turn depends on the rules on the acquisition and transfer of a property right in a digital asset, which in turn depends on establishing that it is conceptually possible and normatively desirable to have a property right in a digital asset. All four of my research questions become relevant even in relatively simple scenarios where a person's use of a digital asset has been interfered with.

It is, of course, understandable that the legal rules on digital assets remain relatively unclear, and this is not only because they are an entirely new asset class. Digital assets represent a complex and technical area that requires an understanding of various disciplines such as computer science and some knowledge of business and/or the financial markets. Yet, it is very important to have clarity about the legal aspects of digital assets, most importantly because (1) digital assets are high value assets that are actively traded between people, and (2) digital assets are frequently the subject of hacks that lead to people being unable to use the digital assets that were previously under their control (or people being unable to use certain functionalities in respect of such digital assets).

---

<sup>39</sup> Although, as will be seen in Chapter 4, Section 4.2, a 'recovery of control' remedy that does not depend on a legal wrong will be proposed.

## 2. Focus of this thesis, and importance of its contribution

This thesis will focus on my four research questions (property, acquisition, transfer, and protection),<sup>40</sup> all of which concern private law aspects of digital assets (and specifically personal property aspects), instead of regulatory aspects.<sup>41</sup>

There exists a significant gap in the case law, as well as the secondary literature and other commentary, in relation to my four research questions. For example, there is no English legislative provision or case law that analyses my second, third or fourth research questions. As for my first research question, there is some case law that discusses the ‘property’ issue in respect of digital assets, but this is mainly only in the context of interlocutory applications, insolvency, and trusts. It does not discuss the underlying content of the property right. This ‘gap’ will be explored in Section 2.2 below.

If there is a lack of legal clarity about the questions I intend to explore in this thesis, then a series of negative consequences would follow. Importantly, users of digital assets would not know their legal positions. This makes it hard for both retail and institutional players to assess their overall legal risk. Such uncertainty could also stifle valuable business deals and discourage the development of further use cases of blockchain technology and digital assets. It could also allow parties to pressure claimants into settling their claims for a low sum.

The lack of clarity about the legal nature of digital assets (including the circumstances under which property rights in respect of digital assets can be acquired and transferred, and the extent of protection offered by such property rights) also makes it difficult for regulators to

---

<sup>40</sup> See n 1 above and text thereto.

<sup>41</sup> By ‘private law’ I am referring to rights between persons, as opposed to ‘regulation’ (rules or laws established by governmental bodies to govern specific activities, industries, or behaviours).

regulate such assets, as they would not be able to accurately assess the legal risks associated with such assets.

Having more clarity about the four research questions creates a significant number of benefits. Most importantly, there would be an increased level of legal certainty as people would have a much better idea of where they stand legally, which in turn would also help individuals and companies with risk assessment, decision making, and planning their affairs. This would also encourage transactions and innovations in the blockchain space, and facilitate new use cases. Furthermore, an increased level of legal certainty would also reduce the chance that a well-resourced individual or company could pressure a less well-resourced individual into settling a claim for a very low sum.

The analysis in this thesis could serve as a point of reference for English courts and Parliament when faced with issues that engage one or more of the four research questions.

Having more clarity about the four research questions can also be useful for other countries in the Commonwealth or countries adopting the common law, as they can use the analysis and positions in this thesis as a potential reference point when considering which rules they want to adopt in relation to the four research questions explored in the thesis. Additionally, as legislation<sup>42</sup> in respect of digital assets is being considered, it is important to proceed on a clear view of the underlying issues.<sup>43</sup>

---

<sup>42</sup> Property (Digital Assets etc) HL Bill (2024-25).

<sup>43</sup> The Bill intends to remove the (actual or perceived) hurdle posed by *Colonial Bank v Whinney* [1885] 30 Ch D 261 (which is often used as authority for the proposition that something cannot be admitted into the category of (personal) property if it is not a chose in action or a chose in possession; see Law Commission of England and Wales, *Digital assets as personal property: Supplemental report and draft Bill* (HC 188, Law Com No 416, 2024), Appendix 2 (draft bill), 2.1), such that (*inter alia*) the decision does not prevent the recognition of property rights in cryptoassets merely because they are not choses in action or choses in possession: 3.1-3.7, 3.24-3.31. The Bill provisions themselves do not address any of my four research questions, but the Bill increases the importance of my four research questions because if it is passed (such that the *Colonial Bank* obstacle is removed), it is imperative for the courts to tackle the fundamental questions instead of peripheral or distracting ones. Examples of the courts not tackling the fundamental questions will be seen in Chapter 1, Section 5 below.

Furthermore, analysing the four research questions can help to develop and deepen one's understanding of property from a theoretical and conceptual perspective. This can shed light on the outer limits of the types of objects that can be the subject-matter of a property right, and can be used as a test for whether the existing theories of property need to be revised or modified to take the digital asset context into account. Also, given that my four research questions involve an examination of whether (and to what extent) the existing rules and principles of personal property law can apply across to digital assets, tackling the four questions can further our understanding of the underlying rationales for the (personal property) rules explored.

As such, my thesis provides an original and significant contribution from both a theoretical and a practical perspective.<sup>44</sup>

## **2.1 Aim, substance, and technique**

Throughout this thesis I draw many analogies with physical assets (and the legal rules governing physical assets), as well as distinctions from them. This is because physical assets form a useful baseline of comparison with digital assets.<sup>45</sup>

Nonetheless, it is crucial to clarify the 'level' at which I am making the relevant analogy or distinction. There are three 'levels' – (1) aim, (2) substance, and (3) technique.

A core aim of a property regime in both the physical and digital asset context is to find the appropriate level of protection for various parties, where the duties imposed are not too onerous, and the rights and powers conferred on people are adequately protective and

---

<sup>44</sup> This thesis considers cases that have been decided (and law journal articles/book chapters that have been published) before 1 September 2024. It also takes into account my own publications after 1 September 2024.

<sup>45</sup> Given that physical assets exist independently from the legal system, are rivalrous, and can be involuntarily alienated or destroyed. Digital assets have these characteristics as well: see Chapter 1, Sections 6.1.2, 6.1.3 and 6.2.1 below.

facilitative. For example, in relation to the protection of use of a claimant's digital asset, imposing duties on defendants means taking away their liberties, and the question arises as to what is the appropriate level of protection to set (and thus what liberties defendants and third parties should be able to retain).

Nonetheless, even if this aim is common to both physical and digital assets, the substance (or threshold) of the rule that best gives effect to such an aim may differ across physical and digital assets (even though the threshold could also be the same). For example, in the case where a defendant impairs the use of the claimant's asset, the mental element that a defendant must have before he interferes with the claimant's property rights may differ across physical and digital assets.<sup>46</sup>

Finally, the doctrinal and conceptual techniques that are used to achieve a particular threshold (or substantive level) of protection may differ across physical and digital assets. This is even if the substance of the rule in the digital asset context is the same as or equivalent to that in the physical asset context. For example, the threshold for acquiring an original title to both a physical and a digital asset could be where one obtains (positive and negative)<sup>47</sup> control of it with the intention to exercise control of it on one's behalf, but the concept or doctrine used to describe such a threshold could be 'possession' in the physical asset context but 'control' in the digital asset context.<sup>48</sup>

Analogies between physical and digital assets can happen at each of the three levels, and an analogy in respect of one level does not necessarily mean that an analogy has to be drawn at another level. There could be an analogy at the 'aim' level but a distinction drawn at

---

<sup>46</sup> This will be explored in Chapter 4: see e.g. Chapter 4, Section 4.2.

<sup>47</sup> The 'positive' and 'negative' dimensions of control will be discussed in Chapter 2 (see e.g. Chapter 2, Section 2.1.1 below).

<sup>48</sup> This is what will be argued in Chapter 2 (in relation to digital assets).

the ‘substance’ and/or ‘technique’ level.<sup>49</sup> There could also be an analogy drawn at the ‘substance’ level but a distinction drawn at the ‘technique’ level.<sup>50</sup>

## **2.2 State of the case law, commentary, and legislation, and what ‘gap’ is to be filled**

As mentioned,<sup>51</sup> there is a ‘gap’ in the current case law insofar as there is no case law that discusses my second, third, or fourth research questions. There was also an extremely significant gap in the literature prior to the Law Commission’s 2023 Final Report and 2022 Consultation Paper on digital assets, and even though the two Law Commission publications have considerably reduced this gap, there remain obvious gaps in the literature in relation to the four research questions.

There has indeed been some case law that explores various ‘property-related’ questions in the digital asset context. For example, some cases have ruled that certain types of cryptoassets can be ‘property’ for the purpose of insolvency, as well as for the purpose of interlocutory applications such as freezing orders and proprietary injunctions, and that (i.e. whatever the property right is in a cryptoasset)<sup>52</sup> can be held on trust.<sup>53</sup>

However, the case law has not explored the logically prior question of what the incidents are of this ‘property’ right that can (arguably) form part of an insolvent’s estate, be held on trust, and be the subject of a freezing order or proprietary injunction. In other words, *what is it* that can be held on trust, and so on?

---

<sup>49</sup> E.g. Chapter 4 (protection) – the aim is analogous (to offer the most appropriate level of protection), but the substance and technique are both different (chattel torts v new regime).

<sup>50</sup> E.g. Chapter 2 (acquisition of a property right) – the substance is analogous (positive and negative control) but the respective techniques used are different (possession v control).

<sup>51</sup> See Section 2 para 2 above..

<sup>52</sup> Which the cases do not clarify: See Chapter 1, Section 5 below.

<sup>53</sup> See Chapter 1, Section 5.1-5.3 below.

Also, insofar as they involve non-interference rights effective against the world, what is the extent to which such rights are effective against third parties? And how should such rights arise (the ‘acquisition’ question), and how should these rights be transferred to another person (the ‘transfer’ question)?

These are crucial questions that have not been explored in the case law and will be investigated in this thesis.

In terms of the literature/commentary on the private law aspects of digital assets it would be useful to distinguish two periods of such commentary: (1) the 2016-2020 period, and (2) the 2021-2024 period. This is because 2021 was the year that the Law Commission published its first substantial paper on digital assets (the Call for Evidence),<sup>54</sup> followed by its Consultation Paper in 2022<sup>55</sup> and its Final Report in 2023.<sup>56</sup> The publication of these documents generated a lot of discussion and commentary, in the form of articles and consultation responses.<sup>57</sup>

The literature in period (1) grappled with various initial questions such as whether cryptocurrencies constitute property from a conceptual perspective,<sup>58</sup> property classification issues,<sup>59</sup> and some trusts and custody issues.<sup>60</sup> The most significant contribution during this stage was the UKJT Legal Statement on cryptoassets and smart contracts, which covered a range of issues such as property, classification, transfer, security, and insolvency.<sup>61</sup> Nonetheless,

---

<sup>54</sup> Law Commission of England and Wales, *Digital assets – Call for evidence* (2021).

<sup>55</sup> Law Commission of England and Wales, *Digital Assets: Consultation paper* (Law Com No 256, 2022).

<sup>56</sup> Law Commission of England and Wales, *Digital Assets: Final report* (HC 1486, Law Com No 412, 2023).

<sup>57</sup> See e.g. Law Commission of England and Wales, *Digital assets Responses to consultation* (2022); Law Commission of England and Wales, *Digital assets Responses to the call for evidence* (2021).

<sup>58</sup> See e.g. UK Jurisdiction Taskforce, *Legal Statement on Cryptoassets and Smart Contracts* (2019) (e.g. at paras 15 and 31-40); Joanna Perkins and Jennifer Enwenzor, ‘The legal aspect of virtual currencies’ (2016) 10 JIBFL 569.

<sup>59</sup> Perkins and Enwenzor (n 58 above), 570.

<sup>60</sup> See e.g. Kelvin FK Low, ‘Quoines in Cryptopia: When (if ever) are Cryptoasset Exchanges Trustees?’ [2020] Conv 70; Kelvin FK Low, ‘Trusts of Cryptoassets’ (2021) 34(4) TLI 191 (article uploaded on SSRN in 2020: see [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3749040](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3749040) (accessed 1<sup>st</sup> January 2025)).

<sup>61</sup> UK Jurisdiction Taskforce (n 58 above).

the depth and coverage of the analysis was relatively limited, in comparison to the period (2), i.e. 2021-24.

The second period was characterised by the publication of the Law Commission’s Call for Evidence, Consultation Paper, and Final Report on digital assets, and the responses and surrounding commentary in relation to these papers/reports. In particular, the Law Commission’s 2022 Consultation Paper and its 2023 Final Report provided an extensive amount of commentary on many private law issues in respect of digital assets – including custody, insolvency, the Financial Collateral regulations, transfer of title, interference, and linked assets.<sup>62</sup> These papers have spawned further commentary, and there is now an increasing body of literature that has discussed these issues, especially in the last two years.<sup>63</sup>

However, the coverage of issues (and depth of analysis) in the literature has not been comprehensive and there are many questions that remain relatively underexplored. This is especially in relation to the acquisition of title question and the interference question, (which, for example, the Law Commission does not explore comprehensively).

---

<sup>62</sup> See e.g. Law Commission, *Consultation paper* (n 55 above), Chapters 11, 13, 14, 16, 17, 18, 19; Law Commission, *Final report* (n 56 above), Chapters 4, 6, 7, 8, 9. Also see discussion of similar issues in the UNIDROIT Principles on Digital Assets and Private Law (published in October 2023) and accompanying commentary.

<sup>63</sup> See e.g. Peter Watts and Kelvin FK Low, ‘The Case for Cryptoassets as Property’ in Sinead Agnew and Marcus Smith (eds), *Law at the Cutting Edge* (Hart Publishing, 2024) 281; Timothy Chan and Kelvin FK Low, ‘Post-Scam Crypto Recovery: Final Clarity or Deceptive Simplicity?’ (2023) 139 LQR 379; Timothy Chan and Kelvin FK Low, ‘DeFi Common Sense: Crypto-backed Lending in *Janesh s/o Rajkumar v Unknown Person* (*CHEFPIERRE*)’ (2023) 86 MLR 1278; Duncan Sheehan, ‘Digital assets, blockchains, and relativity of title’ [2024] JBL 77; Timothy Chan, ‘The nature of property in cryptoassets’ (2023) 43 LS 480; Stevens (n 28 above); Hin Liu, ‘Crypto as property: a response to Professor Stevens’ (2025) 141 LQR (forthcoming); Hin Liu, ‘Interference torts in the digital asset world’ (2025) 84 CLJ (forthcoming).

Nonetheless, many of my arguments in this thesis have influenced the Law Commission's stance,<sup>64</sup> which shows that my research questions have had a practical effect beyond the legal academy, and thus have been worthy of investigation.<sup>65</sup>

On the legislative reform side, the most recent proposal is the draft Property (Digital Assets etc) Bill proposed by the Law Commission, and it is currently being considered by Parliament.<sup>66</sup> However, it does not address any of my four research questions – it merely clears an (actual or perceived) hurdle to the recognition of digital assets as property.<sup>67</sup>

The only legislative provision that deals with the property law aspects of digital assets in a relatively detailed fashion is the Dubai International Financial Centre (“DIFC”)’s Digital Assets Law (“DAL”).<sup>68</sup> The Digital Assets Law contains provisions that cover (*inter alia*) the characterisation of digital assets as property, original acquisition of title to a digital asset, how such title can be transferred, and the interference regime in respect of digital assets.<sup>69</sup>

The content and views of this thesis overlap substantially with the thresholds in the DAL in respect of the acquisition and transfer of a property right, as well as the interference threshold. This is in part because of my involvement in the drafting of the DAL, and many of

---

<sup>64</sup> E.g. my arguments in relation to control (Chapter 2) and interference (Chapter 4). Many of my views in this thesis were formulated and published before the Law Commission Consultation Paper and/or Final Report were published, and a considerable number of them have been adopted or cited by the Law Commission in their Consultation Paper and Final Report: see e.g. Law Commission, *Final report* (n 56 above), 9.72, 9.73, 9.76, 9.46, 9.57, 6.41-6.43; Law Commission, *Consultation paper* (n 55 above), 11.58, 11.86, 11.116. Part of this is because of my role as Advisory Panel member for the Law Commission's Digital Assets project.

<sup>65</sup> Many of the arguments in my thesis have been published (or are forthcoming) as articles or book chapters, and a lot of the text in the thesis is taken directly (often with some modification) from seven of my (existing or forthcoming) publications: Liu, ‘Interference torts’ (n 63 above) (and earlier version of article at <https://ssrn.com/abstract=4433956> (accessed 21<sup>st</sup> December 2024)); Liu, ‘Crypto as property’ (n 63 above); Hin Liu, ‘Transfer of title to digital assets’ in Jason Allen, Simon Gleeson and Peter Hunn (eds), *Oxford Handbook of Digital Assets and the Law* (OUP, 2025) (forthcoming); Hin Liu, ‘Title, control and possession in the digital asset world’ [2022] LMCLQ 597; Hin Liu, ‘Transferring legal title to a digital asset’ (2023) 5 JIBFL 317; Hin Liu, ‘Transferring legal title to a digital asset: shared and limited control arrangements (Part 2)’ (2024) 4 JIBFL 251.

<sup>66</sup> The Bill has completed its second reading in the House of Lords: ‘Property (Digital Assets etc) Bill [HL] – Parliamentary Bills – UK Parliament’, *UK Parliament* at <https://bills.parliament.uk/bills/3766> (accessed 1st January 2025).

<sup>67</sup> See n 43 above.

<sup>68</sup> Dubai International Financial Centre, Digital Assets Law (DIFC Law No. 2 of 2024).

<sup>69</sup> *ibid*, Articles 8-15.

my arguments in this thesis have (to a significant extent) been reflected in the provisions of the DAL.<sup>70</sup>

However, an investigation of the four research questions will also fill gaps left by the DAL Consultation Paper in relation to the acquisition, transfer, and interference questions.

### **2.3 Structure of thesis**

This thesis has four substantive chapters, and each chapter deals with one of the following four questions:

1. Whether digital assets are capable of being the subject matter of a ‘property’ right (in the sense of being the object of non-interference rights exigible against the world), and whether it is normatively desirable to recognise such a property right in a digital asset;
2. How one should acquire such a property right for the first time (and what is the appropriate doctrinal label for the relevant threshold);
3. How such a right should be transferred; and
4. What the general scope of protection should be in relation to this right (i.e. the general boundary of the non-interference right).

---

<sup>70</sup> Of course, in various respects the stance of my thesis deviates from the stance taken in the DAL.

# **Chapter 1: Digital Assets as Property?**

## **1. Introduction**

The ultimate aim of Chapter 1 is to establish that digital assets are capable of being the subject-matter of a property right, and that it is normatively desirable to recognise property rights in digital assets. This will be explored in the final section of this chapter (Section 6).

Sections 2, 3 and 4 will provide clarification on what will be explored. In particular, Section 2 will discuss the meaning of ‘digital asset’ and scope of digital assets that will be explored for this thesis. Section 3 will explore the potential meanings of ‘property’. Section 4 will discuss why non-interference rights in relation to a digital asset is the meaning of ‘property’ explored for the purpose of this thesis, and clarify related matters in relation to ‘title’, ‘ownership’, and the ‘right to exclude’.

In turn, Section 5 will discuss the case law on property-related issues in the digital asset context, including what gap(s) exist in the case law and how this thesis intends to address such gaps.

Having set out the context in Sections 2-5, Section 6 will establish that it is conceptually possible and normatively desirable for property rights to exist in relation to digital assets.

## **2. Meaning of ‘digital asset’**

It would be useful to clarify what the term ‘digital asset’ may mean, and discuss the scope of digital assets that will be covered for the purpose of this thesis.

The term ‘digital asset’ can carry a variety of meanings. For example, it can refer to an asset that uses digital electronics (such as a digital calculator or a digital clock), or assets that

exist on a computer (such as a Word or Excel file). It can also refer to a (factual) power to make transactions on a blockchain or another distributed ledger – which is the meaning on which this thesis will focus.

A distributed ledger is a database that is decentralised and managed by multiple participants, and contains rules that determine whether a proposed entry on the database or ledger is valid (a ‘consensus algorithm’, as mentioned earlier).<sup>1</sup> The most common type of distributed ledger is a blockchain.

A blockchain is a distributed ledger that consists of ‘blocks’ (groups of database entries) that are cryptographically linked (‘chained’) to each other using cryptographic hashes, and grows over time.<sup>2</sup> Each block also has a unique timestamp. Proposed blocks need to be verified by participants in the network as being compliant with the consensus algorithm before they can be added to the ledger, and this helps to ensure the immutability of the data on the blockchain.<sup>3</sup>

This results in a ‘tamper-proof’ ledger,<sup>4</sup> because a unilateral attempt to fraudulently change the entries on the blockchain (e.g. by proposing a block that includes various false transactions that enrich the proposer) will inevitably fail – the participants on the blockchain will be able to detect the false block as it would not conform to the consensus and verification rules of the blockchain.

---

<sup>1</sup> DLT (distributed ledger technology) is “a database of information that [is] shared and duplicated across a network of computers in different locations”: Winston & Strawn, 'What Is Distributed Ledger Technology (DLT)? | Law Glossary | Winston & Strawn', *Winston & Strawn* at <https://www.winston.com/en/legal-glossary/distributed-ledger-technology> (accessed 1st January 2025).

<sup>2</sup> The range of definitions of ‘blockchain’ can vary, but (from my industry experience) this definition would align with how the term is generally used in practice.

<sup>3</sup> See e.g. James Ramsden, ‘Identifying and tracing the origins and flows of cryptocurrency’ (2019) 3 JIBFL 173, 173.

<sup>4</sup> Nonetheless, although “blockchain technology produces a ‘tamper-proof’ ledger”, it can still be subject to hacks and “cyberattacks”: see e.g. 'What Is Blockchain Security? | IBM', IBM at <https://www.ibm.com/topics/blockchain-security> (accessed 1st January 2025).

This raises the question of what a digital asset is. A digital asset, like Bitcoin or Ether, consists of a factual ability to make transactions that alter the entries on a distributed electronic ledger, and this is what David Fox describes as a ‘transactional power’.<sup>5</sup>

Each digital asset (transactional power) is associated with a ‘public key’, an alphanumeric string that denotes the (virtual) location in which the digital asset is located. It can be thought of as the identifier of the ‘vault’ in which the digital asset is ‘stored’.<sup>6</sup> The public key is represented by a ‘public address’, a hashed version of the public key.<sup>7</sup>

The power is exercised by signing a signature using the private key that is associated with the public address in which the digital asset is located. The private key is an alphanumeric string that can be thought of as a ‘password’ to access assets within the ‘vault’, and if a person knows the private key to a public address in which the digital asset is located, then he would have exclusive control over the digital asset.<sup>8</sup>

The primary power is the power to transfer, and (depending on how the digital asset is programmed) it can have other powers such as voting, freezing,<sup>9</sup> minting,<sup>10</sup> claiming an airdrop, or taking an in-game action.

For the purposes of this thesis, I will focus on transactional powers that exist on blockchains, as opposed to all DLT ledgers. At present, the vast majority of DLT assets are held on blockchains. In general however, the analysis in this thesis applies to other types of DLT ledgers as well (such as hashgraphs).

## 2.1 Types of digital assets

---

<sup>5</sup> David Fox, ‘Digital assets as transactional power’ (2022) 1 JIBFL 3.

<sup>6</sup> See e.g. Hin Liu, ‘Title, control and possession in the digital asset world’ [2022] LMCLQ 597, 599; Hin Liu, ‘The legal nature of blockchain securities’ [2021] LMCLQ 476, 479 (fn20).

<sup>7</sup> The public address, like the public key, is an alphanumeric string.

<sup>8</sup> Assuming no one else knows the key (and in practice there is little chance this is not going to be the case): see UNIDROIT Digital Assets and Private Law Commentary 7.2.

<sup>9</sup> Disabling someone from being able enter transactions in respect of a digital asset, or (at minimum) disabling someone from being able to transfer a digital asset out of its address.

<sup>10</sup> Creating a new digital asset.

Digital assets can be sorted in various ways, and it would be helpful to explore some key distinctions that help to set out the various types of digital assets.

The first distinction is between ‘native’ and ‘linked’ digital assets. Native assets are assets on a blockchain that do not represent another asset and purely exist within their own system.<sup>11</sup> Examples include Bitcoin and Ether.

Linked assets, on the other hand, are assets on a blockchain that in some way ‘represent’ another asset.<sup>12</sup> The underlying asset to which the digital asset is linked could be, for example, a debt, a share, or a physical asset. There are various types of ‘links’, two of which are most significant. First, there could be a ‘constitutive’ link between the digital asset and the underlying asset, i.e. the person who has the digital asset holds the relevant right to the underlying asset.<sup>13</sup> Second, there could be an ‘evidential’ link, where if a person has the digital asset, this is evidence that he holds the relevant right to the underlying asset.<sup>14</sup> The strength of the ‘evidential’ link may vary from asset to asset, and an example of a digital asset with a strong ‘evidential’ link would be tokenised share certificates.<sup>15</sup>

The analysis in this thesis will apply to both native and linked digital assets. However, this thesis will not explore the nature and content of the ‘link’ between the digital asset and the relevant asset to which it is ‘linked’.<sup>16</sup>

Second, there is a distinction between permissionless and permissioned blockchains. Permissionless blockchains are blockchains that anyone can read (view) and write to (enter transactions on). Permissioned blockchains are blockchains where there are restrictions on

---

<sup>11</sup> Liu, ‘Blockchain Securities’ (n 6 above), 481.

<sup>12</sup> *ibid*, 481.

<sup>13</sup> Hin Liu, ‘Digital assets: the mystery of the “link”’ (2022) 3 JIBFL 161, 161-162.

<sup>14</sup> *ibid*, 161-162.

<sup>15</sup> *ibid*, 161-162.

<sup>16</sup> I have explored linked assets in previous articles (see Liu, ‘Mystery of link’ (n 13 above); Liu, ‘Blockchain Securities’ (n 6 above)).

access and participation (i.e. where only authorised participants can read and write to the ledger).<sup>17</sup> For the purpose of this thesis, I will limit my discussion to assets on permissionless blockchains.<sup>18</sup>

Third, digital assets can also be distinguished based on their level of transferability. The vast majority of digital assets are programmed to be capable of being transferred to other addresses.

However, a digital asset can also be programmed from the outset to be (permanently) incapable of being transferred to other addresses. Most obviously, this can be done through not adding a ‘transfer’ function into the code that governs the digital asset, meaning that there is no programmed capability to transfer the asset into a different address.<sup>19</sup>

Digital assets that are programmed from the outset to be non-transferable will not be explored in this thesis. Only a very small minority of digital assets fall into this category – for example debt tokens in Aave v2/v3, which are intended to track liabilities.<sup>20</sup>

It is important to distinguish digital assets that are inherently programmed at the outset to be non-transferable, and digital assets that are programmed to be transferable but are currently in an address where there are restrictions on transfer. For example, if a digital asset is transferred into a smart contract address that restricts the ability to transfer until certain conditions are satisfied<sup>21</sup> (e.g. in the context of escrow agreements), the asset is *currently* non-transferable but is not programmed to be *inherently* non-transferable. Once the relevant condition is satisfied, the ability to transfer the asset will be restored. Thus, the analysis in this

---

<sup>17</sup> 'Types of Blockchain – GeeksforGeeks', *GeeksforGeeks* at <https://www.geeksforgeeks.org/types-of-blockchain/> (accessed 1 January 2025).

<sup>18</sup> Permissioned blockchains may involve an extra layer of complexity as there may be a multilateral contractual framework (see e.g. Law Commission of England and Wales, *Digital Assets: Consultation paper* (Law Com No 256, 2022), 10.103), which this thesis has no space to explore.

<sup>19</sup> See e.g. *ibid*, 10.130.

<sup>20</sup> *ibid*, 10.130.

<sup>21</sup> Which could be time-based, act-based or event-based: see Chapter 3, Section 8.3.4.

thesis will also apply to digital assets that are currently non-transferable but are not inherently so.

## **2.2 Summary of digital assets explored in thesis**

To summarise, the ‘digital assets’ that will be covered in this thesis are permissionless blockchain assets that are not programmed from the outset to be (permanently) non-transferable, and involve a power to alter the entries of a public blockchain ledger. Examples of such assets include Bitcoin, Ethereum and Solana, as well as tokens on created on the Ethereum and Solana blockchains that are not programmed from the outset to be (permanently) non-transferable. Tokens created on such blockchains<sup>22</sup> can be (e.g.) NFTs, DAO tokens, security tokens,<sup>23</sup> as well as utility tokens.<sup>24</sup>

## **3. Meaning of ‘property’**

Having clarified what my scope of inquiry is in relation to ‘digital assets’, the next question to ask is whether the digital assets I will be exploring constitute property. In this regard, it is important to clarify which meaning of property is being used for the purpose of this thesis. ‘Property’ can carry a wide range of meanings, and five will be explored, with a view to determining which one would lead to the most fruitful discussion for the purpose of this thesis.

The five meanings have been selected not just because of their potential relevance to digital assets. They have also been selected because of their prominence in the literature and/or case law, as well as their theoretical, conceptual, practical or legislative significance. The

---

<sup>22</sup> And are not programmed from the outset to be non-transferable.

<sup>23</sup> Digital assets that represent securities or rights thereto.

<sup>24</sup> Digital assets that can be used for accessing a product or service.

overall aim is not to ascertain what the ‘best’ interpretation of property is, but rather to examine which interpretation provides questions that are most useful to ask for the purpose of the thesis.

### **3.1 Meaning 1: Realisable commercial value**

First, Roy Goode uses the term ‘property’ to mean anything with realisable commercial value (subject to statute).<sup>25</sup> Digital assets of course have realisable commercial value, as evidenced by (e.g.) the prices of various highly traded digital assets,<sup>26</sup> which are being quoted in real time on exchanges such as Binance and Coinbase. There is no real debate as to whether digital assets satisfy this meaning of property, and in addition, being within the definition has no necessary legal consequences. For example, the fact that a digital asset has realisable commercial value does not provide any indication as to whether there are rights to sue for interference in the case of a hack, or whether there is a power to transfer any right(s).

As such, it is not particularly interesting or fruitful to discuss whether digital assets are property under this meaning.

### **3.2 Meaning 2: Non-interference rights**

The term ‘property’ could also be used to refer to non-interference rights in relation to the asset in question that are exigible against the world, or particular types of these rights. These rights correlate to non-interference duties imposed on the rest of the world.

---

<sup>25</sup> Sir Roy Goode QC, ‘What is property?’ (2023) 139 LQR 1, 4.

<sup>26</sup> Such as Bitcoin (worth approximately \$93,000 as of 1<sup>st</sup> January 2025) and Ether (worth approximately \$3,300 as of 1<sup>st</sup> January 2025): see e.g. ‘Cryptocurrency Prices, Charts And Market Capitalizations | Coinmarketcap’, *Coinmarketcap* at <https://coinmarketcap.com> (accessed 1 January 2025).

For example, Smith notes that the “traditional definition of property is a right to a thing good against the world”.<sup>27</sup> If there are rights in respect of an object (thing) that are exigible against the world, then people are under duties in relation to the relevant object.<sup>28</sup> In the context of chattels and land (the most traditional forms of ‘things’), this encompasses a duty not to interfere with the thing, and/or its use, in particular circumstances.<sup>29</sup>

Similarly, according to Merrill, “the right to exclude others is a necessary and sufficient condition for identifying the existence of property”.<sup>30</sup> The right to exclude others from a particular asset consists of non-interference rights that are effective against the world – if one can sue any person for (non-consensually) interacting with or interfering with the object, this amounts to a series of non-interference rights that are effective against the world.<sup>31</sup>

Also, McFarlane and Douglas note that the special feature of a property right lies in the duties it imposes on the rest of the world, and not the positive uses that it affords.<sup>32</sup> They explore this question in the physical asset context, and they conclude that the package of rights (under the torts of conversion, trespass, and negligence (for chattels) and the torts of trespass to land and nuisance (for land)) involves a right that others do not interfere with the thing.<sup>33</sup>

Furthermore, Stevens in a recent article discussing cryptoassets<sup>34</sup> notes that one sense in which common lawyers use the word ‘property’ is to mean rights to a physical thing that are exigible against the world.<sup>35</sup>

---

<sup>27</sup> Henry Smith, ‘Property as the Law of Things’ (2012) 125 Harv LR 1691, 1706.

<sup>28</sup> Claim-rights and duties are Hohfeldian jural correlatives, such that if X has a claim right against Y (or the world), then Y (or the world) owes a duty to X.

<sup>29</sup> Or usability. See n 174 below.

<sup>30</sup> Thomas W Merrill, ‘Property and the Right to Exclude’ (1998) 77 Neb L Rev 730, 731.

<sup>31</sup> Nonetheless, there are various possible meanings of the ‘right to exclude’, which will be explored in Section 6.2.2 below.

<sup>32</sup> Simon Douglas and Ben McFarlane, ‘Defining Property Rights’ in James Penner and Henry Smith (eds), *Philosophical Foundations of Property Law* (OUP, 2013) 219; 219-220, 224; Ben McFarlane and Simon Douglas, ‘Property, Analogy and Variety’ (2022) 42 OJLS 161, 169-170.

<sup>33</sup> Douglas and McFarlane (n 32 above), 219, 226, 220; McFarlane and Douglas (n 32 above), 165.

<sup>34</sup> Robert Stevens, ‘Crypto is not property’ (2023) 139 LQR 615.

<sup>35</sup> *ibid*, 616.

Though this meaning focuses on *physical* things, it is suggested that the abstract structure of rights (non-interference rights in respect of an object/thing) is not limited to physical assets. Indeed, much of the commentary on digital assets proceeds on the basis that there can (from a conceptual perspective) be non-interference rights in respect of a digital asset that are exigible against the world,<sup>36</sup> and it will be shown later in this chapter<sup>37</sup> that this is the case because of the characteristics of a digital asset.

A common view is that the core purpose of non-interference rights in respect of a thing or object is to protect the use of that thing or object. Smith for example notes that “Rights to exclude are a means to an end, and the ends in property relate to people’s interests in using things”.<sup>38</sup> Similarly, Merrill and Smith make the point that giving people rights of exclusion in respect of a thing helps to protect “a possessor or owner’s use in using a cluster of attributes”<sup>39</sup> in respect of that thing.<sup>40</sup>

Brown and Pawlowski also note that “the ‘use’ of property serves as a justificatory role for the property right while ‘exclusion’ is the formal essence of the right.”<sup>41</sup>

In the digital asset context, the package of non-interference rights exigible against the world that should be imposed is highly worthy of exploring, because of its practical significance. There are many ways in which a digital asset (or its use) can be interfered with,<sup>42</sup> and digital assets are being used and traded very frequently on a daily basis (e.g. the daily

---

<sup>36</sup> See e.g. Law Commission of England and Wales, *Digital Assets: Final report* (HC 1486, Law Com No 412, 2023), 9.61-9.83; Sarah Green and Ferdisha Snagg, ‘Intermediated Securities and Distributed Ledger Technology’, in Louise Gullifer and Jennifer Payne (eds), *Intermediation and Beyond* (Hart Publishing, 2019) 337, 345-348 (DLT cryptosecurities); Hin Liu, ‘Interference torts in the digital asset world’ (2025) 84 CLJ (forthcoming); Hin Liu, ‘Crypto as property: a response to Professor Stevens’ (2025) 141 LQR (forthcoming).

<sup>37</sup> In Sections 6.1 and 6.2 below.

<sup>38</sup> Smith (n 27 above), 1704.

<sup>39</sup> Thomas W Merrill and Henry E Smith, ‘The Architecture of Property’ in Hanoeh Dagan and Benjamin C Zipursky (eds), *Research Handbook on Private Law Theory* (Edward Elgar Publishing, 2020) 134, 143.

<sup>40</sup> This is part of a broader point that both ‘exclusion’ and ‘governance’ strategies can protect use: *ibid*, 143-144.

<sup>41</sup> James Brown and Mark Pawlowski, ‘The Challenge of Identifying Private Property under English Law’ (2022) 86 Conv 305, 305, citing J.E. Penner, *The Idea of Property in Law* (OUP, 1997), Chapter 4.

<sup>42</sup> E.g. via smart contract hacks, DDoS attacks, and using someone’s private key to execute unauthorised transactions.

trading volume in relation to digital assets is over 100 billion).<sup>43</sup> It would be valuable to investigate the extent to which the use of digital assets should be protected (and this extent is reflected via the scope of the non-interference rights).

Also, an analysis of the duties that can and should be imposed on the world (i.e. the correlative of the non-interference rights) reveals the extent to which the policies and concerns in relation to other assets (specifically physical assets, debts, and pure information) about imposing (or not imposing) such duties on the rest of the world apply to digital assets. It also requires reflection on the reasons why protection is given in relation to physical assets. This in turn would also allow one to gain further insight about the nature of the existing protective regime in relation to the other (non-digital) assets.

Regardless of whether people see property as non-interference rights effective against the world (or particular types of such rights), many people accept that non-interference rights effective against the world in respect of a thing is a *necessary* condition of property.<sup>44</sup>

If some people do not accept that this is a sufficient condition of property, what can the ‘missing ingredient’ be? This brings us to the third meaning of property.

### **3.3 Meaning 3: Non-interference rights plus powers**

The third meaning of property refers to non-interference rights exigible against the world coupled with power(s) that one can exercise in respect of such rights.<sup>45</sup>

---

<sup>43</sup> See Introduction, Section 1 (n 38) above.

<sup>44</sup> Thomas W Merrill and Henry E Smith, ‘The Property/Contract Interface’ (2001) 101 *Colum L Rev* 773, 777, 790; Penner (n 41 above), 71-78, 80-90; JW Harris, *Property and Justice* (OUP, 2002), 24-25; Merrill (n 30 above), 730 (right to exclude as “sine qua non”); Adam Mossoff, ‘What is property? Putting the pieces back together’ (2003) 45 *Ariz L Rev* 371, 379-390.

<sup>45</sup> The powers (in respect of the relevant rights) that must exist to constitute ‘property’ are different from person to person.

Penner, for example, uses ‘property’ to mean non-interference rights exigible against the world plus the power to alienate such a right and the power to licence (release third parties from the non-interference duties).<sup>46</sup> Penner treats the powers as part of his definition of property, such that the non-interference rights are not sufficient to constitute property.

Likewise, Rostill uses the term ‘general property interest’ to denote the package of rights and powers that one acquires through taking possession of a chattel.<sup>47</sup> This encompasses non-interference rights against the world (a right to exclusive possession) in respect of the chattel, as well as certain powers, such as the power to transfer the right to another person *inter vivos* or by will.<sup>48</sup> Other powers include the power to create a trust or charge over the right.<sup>49</sup>

Of course, the non-interference rights and the power(s) in respect of them are analytically independent – a legal system can choose to have the former without having the latter, or to have the former but only have some of the latter. For example, in the *Yearworth*<sup>50</sup> case, the claimants had non-interference rights in respect of sperm<sup>51</sup> but did not have the power to alienate such rights to another person.<sup>52</sup>

The powers in respect of the non-interference rights are also highly worthy of investigation because they determine what a person with a non-interference right can do with the right (apart from sue people for interference). For example, the conditions under which one ought to be able to create a trust or charge over the non-interference right, or to alienate the right *inter vivos* or by will, has significant implications in the commercial world (such as in the contexts of custody and succession), and directly impacts party autonomy. It also carries

---

<sup>46</sup> Penner (n 41 above), 68-90; Luke Rostill, ‘The Pluralities of Property’ (2024) 44(3) OJLS 733, 736-737; JE Penner, *Property Rights: A Re-Examination* (OUP, 2020), 14.

<sup>47</sup> Luke Rostill, *Possession, Relative Title, and Ownership in English Law* (OUP, 2021), 112-113. Note however, that this is an account of a particular type of proprietary interest (or ‘property right’) that one can have in respect of chattels under English law, as opposed to an account of the nature of property rights in general.

<sup>48</sup> *ibid*, 100.

<sup>49</sup> These powers are not mentioned explicitly by Rostill, but these are some of the powers that exist as part of a ‘general property interest’.

<sup>50</sup> *Yearworth v North Bristol NHS Trust* [2009] EWCA Civ 37, [2010] QB 1.

<sup>51</sup> In negligence: see e.g. *ibid*, [45](f) and [41].

<sup>52</sup> See e.g. *ibid*, [45](f)(iv).

considerable theoretical and doctrinal significance since it sheds light on whether the existing rules on (e.g.) the creation of trusts and charges can apply across to digital assets, or whether modifications (or a wholly different set of rules) would be required to accommodate the digital asset context.

### **3.4 Meaning 4: Satisfying the conditions in *Ainsworth***

‘Property’ has also been meant in a fourth sense, i.e. a right that satisfies the four conditions set out under *National Provincial Bank v Ainsworth*.<sup>53</sup> The conditions are (1) definability, (2) identifiability by third parties, (3) capability in their nature of assumption by third parties, and (4) some degree of permanence or stability.<sup>54</sup>

This meaning of ‘property’ has been used in many cases that concern digital assets. Specifically, in determining whether cryptoassets constitute property for the purposes of interim applications, insolvency, and trusts,<sup>55</sup> judges in a number of cases have applied and/or referred to the *Ainsworth* test (as will be shown in Section 5.1-5.3 below).<sup>56</sup>

The *Ainsworth* conditions have been criticised in the literature as not being a good test for whether something should be admitted into the category of ‘property’.<sup>57</sup> Indeed, it is suggested that the *Ainsworth* conditions are not very meaningful to explore, because they are merely necessary conditions for some right to have some third party effect as opposed to just being a personal right (e.g. a contractual licence).<sup>58</sup> Lord Wilberforce was not defining property

---

<sup>53</sup> *National Provincial Bank v Ainsworth* [1965] AC 1175.

<sup>54</sup> *ibid*, 1248.

<sup>55</sup> Whether a cryptoasset is capable of being the subject-matter of trust.

<sup>56</sup> See Sections 5.1-5.3 below.

<sup>57</sup> Stevens (n 34 above), 622; Kevin Gray and Susan Francis Gray, *Elements of Land Law* (5th ed, Oxford 2009), 97; Kelvin FK Low, ‘Trusts of Cryptoassets’ (2021) 34(4) TLI 191; Kelvin FK Low, ‘Quoines in Cryptopia: When (if ever) are Cryptoasset Exchanges Trustees?’ [2020] Conv 70.

<sup>58</sup> Stevens (n 34 above), 622.

or intending to define it, and on the facts of the case, he was merely providing reasons why a deserted wife's equity should not have third party effect.<sup>59</sup>

It is suggested that exploring whether digital assets meet the four conditions under *Ainsworth* is not very illuminating because doing so does not shed light on the content of the relevant right. Indeed, the test in *Ainsworth* presupposes one knows the content of the right being evaluated. Insofar as that is known, *Ainsworth* then provides a set of necessary conditions for that right to have third party effect as opposed to just being a personal right. However, insofar as the content of that right is unknown, *Ainsworth* does not provide any guidance as to what the right can be. As even the basic question of what non-interference rights can and should arise in respect of a digital asset has not been clarified as of yet, it is suggested that it is much more fruitful to answer these questions first.<sup>60</sup>

### 3.5 Meaning 5: Insolvency

'Property' can also be used to mean what is part of a person's insolvent estate under Section 436 of the Insolvency Act 1986. This can include any transferable rights, powers, liberties or immunities.<sup>61</sup>

In the digital asset context, the question is whether digital assets can be the subject-matter of any rights, powers, liberties or immunities that can form part of an insolvent person's estate.

---

<sup>59</sup> "The wife's right has none of these qualities, it is characterised by the reverse of them": *Ainsworth* (n 53 above), 1248.

<sup>60</sup> The misapplication of the *Ainsworth* test will be discussed in Sections 5.1-5.4 below when discussing the case law on digital assets.

<sup>61</sup> "Property" is defined as follows under s.436: "property" includes money, goods, things in action, land and every description of property wherever situated and also obligations and every description of interest, whether present or future or vested or contingent, arising out of, or incidental to, property". This includes things that would count under *Ainsworth* as purely personal rights. It is a very wide definition, as noted in *Bristol Airport Plc v Powdrill* [1990] BCC 130, 148; see also discussion in Michael Bridge, Louise Gullifer, Kelvin Low and Gerard McMeel, *The Law of Personal Property* (3<sup>rd</sup> edition, Sweet and Maxwell 2021), 1-078.

Liberties and immunities are not relevant because digital assets do not exist within the backdrop of a prohibitive legislative rule, unlike (e.g.) EUA carbon trading allowances,<sup>62</sup> or waste management licences.<sup>63</sup> EUA allowances and waste management licences operate within a legislative rule that prohibits certain conduct (e.g. emitting carbon, or producing pollution based on certain types of waste) – they allow a person to do what is otherwise prohibited by the law. In the digital asset context, there is no relevant prohibitive legislative rule or (*a fortiori*) any specific permission or liberty that exists within such a rule.

As for rights, there are some rights in relation to digital assets that can of course exist and are therefore not interesting to investigate, such as contractual rights in respect of a digital asset. This thesis is concerned with the debate over whether certain types of right can and should exist in respect of digital assets, and there is no such debate as far as contractual rights are concerned.

The fundamental category of rights to investigate in relation to digital assets are non-interference rights effective against the world – and this is explored under meaning 2. The powers associated with such rights are explored under meaning 3.

It would also be interesting to investigate whether there can be equitable rights (such as trusts and charges) in respect of the aforementioned non-interference rights (or the non-interference rights plus the associated powers) that form part of an insolvent's estate, as well as the conditions under which such a right can be created. For example, it would be worth investigating whether the conditions under which one can create a valid trust or charge in respect of (non-interference rights to) digital assets.<sup>64</sup> This is very important because lots of transactions in the institutional and retail spaces involve the management and lending of digital assets, and people need to know where they stand.

---

<sup>62</sup> See Section 6.1.3 below.

<sup>63</sup> *Re Celtic Extraction Ltd* [2001] Ch 475.

<sup>64</sup> Assuming there can be non-interference rights in respect of digital assets.

## 4. Non-interference rights

This thesis will focus on the second meaning of property (non-interference rights exigible against the world).

### 4.1 Meaning 2 v Meaning 3

The main focus of this thesis is on the second meaning, and not the third meaning (non-interference rights plus associated power(s)), for the following reasons.

First, non-interference rights serve as the foundation to protecting people's use of digital assets, and it is necessary to devote a lot of space towards exploring this question. Indeed, people have expectations of being able to exercise the transactional powers associated with a digital asset, and often pay substantial sums as a result of these expectations. These expectations need to be protected via non-interference rights.<sup>65</sup> Correlatively, it is important for third parties to know the extent of their duties to the right-holders.

Also, without non-interference rights effective against the world, there would be a substantially higher risk of a 'free-for-all' where there are far fewer disincentives against perpetrating blockchain hacks and misappropriations, as will be explored in Section 6.3.2 below.<sup>66</sup> The risk of a 'free-for-all' must be minimised in order to protect people's use and peaceful enjoyment of digital assets – and non-interference rights effective against the world are what would help most in achieving this outcome.

---

<sup>65</sup> See Section 6.3.1 below.

<sup>66</sup> See Section 6.3.2 below.

Thus, significant time and space in the thesis needs to be devoted to exploring the nature of the non-interference rights effective against the world (and whether such are conceptually possible in the first place), the normative desirability of having such right, how such rights should be acquired, and general principles about the appropriate scope of such rights (i.e. the appropriate scope of protection afforded against interferences).

Second, non-interference rights are a necessary and fundamental component of meaning 3 (non-interference rights plus powers in respect of them), because the powers are ‘built on top of’ the rights. Research on the non-interference rights will lay the foundation towards further research on the various powers (transfer, licence, trust, charge etc).

Third, if one establishes that it is conceptually possible to have non-interference rights in respect of a digital asset, it would be conceptually possible to have powers in respect of such rights. Indeed, where there is a particular claim right (or set of claim rights) in respect of an asset, there is no conceptual obstacle<sup>67</sup> to recognising the power to transfer such a right or the power to create a trust or charge in respect of it. This is the case for debts, and rights in respect of physical things. It is also the case for non-interference rights in respect of a digital asset.

For example, in relation to a power to alienate the right to someone else (by way of title transfer), there is no obstacle because the law just needs to know who has the right. The law can set out the conditions under which the right-holder changes (e.g. a change of control plus an intention to transfer title).<sup>68</sup>

The same is the case for the power to create a trust or a charge: the law just needs to know who has the equitable interest under the trust or charge, and can set out the conditions

---

<sup>67</sup> As distinct from normative obstacles: see Section 6.3 below. It might still be normatively objectionable to introduce rights that can conceptually exist in relation to an asset.

<sup>68</sup> E.g. this would be the default rule for inter vivos transfers of title in relation to digital assets under DIFC law: see DAL Article 12(1).

under which the claim-right is subject to a trust or charge. As long as there is a claim right in respect of an asset, it can be held on trust or be the subject of a charge.<sup>69</sup>

Yet, it is necessary to have enough clarity on the foundational principles relating to the non-interference rights, before a discussion of the relevant powers becomes most useful. Limitations of space mean that a discussion of the different powers in addition to the non-interference right would result in an insufficiently thorough discussion.

Nonetheless, although the focus of this thesis is on meaning 2 (non-interference rights), there will be a full chapter devoted to discussing one power – namely the power to alienate (or transfer) the non-interference right.

Additionally, there will also be some brief discussion of trusts in Chapter 2 when discussing the mental requirement for the acquisition of original title, as well as some brief discussion of charges in Chapter 3 when considering the control-title inference, and policies in relation to the prevention of fraud and defeated expectations.<sup>70</sup>

For the purpose of Chapters 2 to 4, I am proceeding on the assumption that there is a good normative case for recognising the power to alienate the non-interference rights, along with the power to create a trust or charge. Given that I establish (in Section 6.3) that it is normatively desirable to have non-interference rights, and since non-interference rights tend to be accompanied by such powers, it would be reasonable to assume that there is a good normative case for the non-interference rights being accompanied by such powers.<sup>71</sup> The

---

<sup>69</sup> A claim-right in respect of an *asset* can be subject to a duty (e.g. under a trust or charge), unlike (e.g.) a right not to be falsely imprisoned.

<sup>70</sup> There is also a footnote in Chapter 4 that discusses (what is in substance) the power to confer licences, in the context of the ‘recovery of control’ remedy (see Chapter 4, n 275 below). Here, a claimant (C) has a property right to a digital asset and is trying to recover control of the asset from a defendant (D), and it is suggested that D would have a defence if someone (X) with a property right that is superior to C’s consents to D taking control of the digital asset (and thus exercises his power to release D from his duty to C, or power to confer a licence on D).

<sup>71</sup> For arguments in favour of powers to alienate, create a trust and create a charge, see Liu, ‘Crypto as property’ (n 36 above).

question of whether it is normatively desirable to recognise these powers will not be explored in this thesis.

## 4.2 Meaning 2 v Meaning 5

Exploring meaning 2 is also preferable, for the purposes of this thesis, to exploring meaning 5 (property for the purpose of insolvency). This is because the vast majority of assets that are recognised as property for the purpose of insolvency are *rights*, yet it is not clear which *rights* can or should arise in respect of a digital asset. Thus, it would be most fruitful to discuss the more fundamental question of what rights (non-interference rights)<sup>72</sup> can arise in respect of a digital asset. Once the content of these rights has been ascertained, the question of whether such rights (and further rights) can constitute property for the purpose of insolvency can be tackled in a systematic and thorough way.

In relation to equitable interests, it is suggested that there is not enough space in the thesis to explore them in depth. This is because equitable interests are ‘parasitic’ (or dependent) on the underlying right in respect of digital assets.<sup>73</sup> Any discussion of equitable interests in the digital asset context therefore presupposes that we know what is the right over which the relevant equitable right (trust or charge etc) exists.

The content of the ‘base’ right needs to be explored in sufficient depth before there can be a meaningful discussion of the equitable interest(s) in respect of such a right. The first and most fundamental ‘base’ right is the non-interference right because of its centrality in protecting someone’s ability to use their digital asset, and this is what will be explored. Much time needs

---

<sup>72</sup> Non-interference rights will be explored because of their centrality in protecting the use of digital assets.

<sup>73</sup> There needs to be an underlying right which the equitable interest exists in respect of: see Ben McFarlane and Robert Stevens, ‘The Nature of Equitable Property’ (2010) 4 J Eq 1.

to be devoted to this, and there is not enough space in the thesis to explore equitable interests in enough detail (e.g. the creation of (and transfer of interests under) a trust or charge).

Henceforth, ‘property right’ will denote property under meaning 2 (non-interference rights).

### **4.3 Discussion of title, ownership, and the right to exclude**

One may wonder whether, given the focus of this thesis will be on non-interference rights, whether there will be any substantial discussion on the scope of ‘title’, ‘ownership’, or the ‘right to exclude’.

#### ***4.3.1 Title and ownership***

As my thesis will focus on the non-interference right (and how, if it can and does exist in relation to digital assets, it can be acquired and transferred, as well as general principles as to its scope), any in-depth discussion of the scope (and potential meanings) of ‘title’ or ‘ownership’ would not be material to the focus of my thesis.<sup>74</sup> Thus, the ways in which ‘title’ and ‘ownership’ will be used in this thesis will be stipulated in advance.

I will be using a specific meaning of ‘title’ in the context of chattels. ‘Title’ in the context of chattels will be used to refer to the interest that is acquired when one takes possession of a chattel – i.e. the package of non-interference rights plus the relevant powers in respect of them that is conferred when one takes possession of a chattel. As mentioned earlier, this is what

---

<sup>74</sup> Also, ‘title’ and ‘ownership’ can mean a range of things and most often means more than just the claim rights (i.e. including the powers to alienate, create a trust or charge, etc).

Rostill refers to as a ‘general property interest’.<sup>75</sup> I will use the same meaning (i.e. such a package of rights and powers) in the context of land.<sup>76</sup>

In relation to digital assets, I will use ‘title’ to refer to a property right in a digital asset combined with the powers in respect of such a right that a title-holder in relation to chattel would have. Thus, ‘title’ to a digital asset encompasses non-interference rights exigible against the world, the power to alienate such a right, the power to create a trust and charge over such a right, and so on.<sup>77</sup>

An important point to note is that the property right that is the focus of this thesis (property under meaning 2) is a subset of ‘title’.<sup>78</sup> This is the case in relation to both chattels and digital assets.

I will make extensive references to ‘title’ in Chapters 2 and 3. In Chapter 2, I draw analogies between the threshold and justifications for (a) conferring an original title in respect of a chattel, and (b) conferring an original property right (in the sense of meaning 2) in relation to digital assets.<sup>79</sup> In Chapter 3, I discuss the existing literature/commentary on transferring title to a digital asset in considerable detail, and make extensive reference to the existing rules on transferring title to a chattel, in considering what the appropriate rule should be for transferring a property right to a digital asset.<sup>80</sup>

---

<sup>75</sup> See nn 47-49 above and text thereto.

<sup>76</sup> Of course, in the land context, the interest is not called a ‘general property interest’ but a ‘fee simple estate’: Rostill (n 47 above), 54 (and Chapter 4 generally).

<sup>77</sup> ‘Title’ to a digital asset has a different content to a general property interest in a chattel (e.g. in relation to the boundaries of the non-interference right, or the conditions that need to be met to exercise the power to alienate it). However, the contents of the two are similar enough to justify using the same term of ‘title’ (given that there are non-interference rights, and powers to alienate, create a trust and charge, and so on).

<sup>78</sup> As they are the claim rights that someone who has ‘title’ to an asset has.

<sup>79</sup> Insofar as the general threshold and justifications for conferring an original title to a physical asset are thought to apply to conferring an original title to a digital asset, they would also apply to conferring an original property right in a digital asset (since the incidents of an original property right are a subset of the incidents of an original title).

<sup>80</sup> See e.g. Chapter 3, Sections 5-8.

Also, in Chapters 2 and 3, I will make references to ‘title’ in the context of the ‘control-title’ inference in relation to digital assets.<sup>81</sup> In essence, if X has control of a digital asset, people will generally make the inference that he also has title to the digital asset, and not just that he has non-interference rights exigible against the world in respect of the digital asset – e.g. people will make the inference that he can also transfer such non-interference rights to another person via a sale. Thus, it is necessary to distinguish between ‘property right’ and ‘title’ in the context of digital assets.

In turn, I will use ‘ownership’ to denote the best title in relation to an asset – with ‘title’ used in the sense described above.

#### ***4.3.2 The ‘right to exclude’***

This thesis will also not explore the possible meanings of the ‘right to exclude’ in detail. Insofar as ‘right to exclude’ is synonymous with a property right in the sense of meaning 2, I will just use the term ‘property right’. The ‘right to exclude’ will only be briefly touched upon in Section 6.2.2 of this chapter, where I note that the term ‘right to exclude’ can be used to represent Positions 1-3 in relation to the possible scope of the non-interference right.<sup>82</sup>

## **5. The case law**

Having clarified the meanings of ‘digital asset’ and ‘property’ to be explored for the purpose of this thesis, it would now be appropriate to discuss whether the existing case law has

---

<sup>81</sup> See e.g. Chapter 2, Section 2.2.3 below and Chapter 3, Sections 3.1-3.3 and 8.1 below.

<sup>82</sup> See Section 6.2.2 below.

discussed property-related issues (in a general sense, instead of the sense meant for the purpose of this thesis) in private law that concern digital assets.

There have been many recent private law cases that concern digital assets, many of which state that digital assets (or more precisely, certain types of them) are “property”. However, none has explored the content of the property right (i.e. the non-interference rights) in respect of a digital asset. Nor has any case explored the questions of how to acquire or transfer a property right in a digital asset.

Many of the cases concern interim applications, and the ‘property’ aspect becomes relevant to a person applying for an interim order who is attempting to establish whether digital assets are ‘property’ that can be subject to an interim order such as a freezing order or proprietary injunction.

The cases that do not concern interim applications are predominantly cases that concern insolvency as well as breaches of contract and trust.

In this section, I will discuss some cases involving (1) interim applications, (2) insolvency, as well as (3) other issues relating to trusts and contracts.<sup>83</sup>

## **5.1 Interim applications cases**

A group of cases concern whether digital assets are ‘property’ for the purpose of interim applications,<sup>84</sup> and I will focus on the case of *AA v Persons Unknown*.<sup>85</sup>

*AA* contains a considerable amount of analysis on the ‘cryptoasset as property’ issue in the context of proprietary injunction applications. In *AA*, Bitcoin was paid by the claimant as a

---

<sup>83</sup> There are, of course, more cases in each category, but many of them address points that are similar to the points explored below. One key case in category (1) will be explored, and two key cases in (each of) categories (2) and (3) will be explored.

<sup>84</sup> For the purpose of the discussion below, I will ignore the conflict of laws issues discussed in the cases as they are not directly relevant to my thesis.

<sup>85</sup> [2019] EWHC 3556 (Comm).

result of a ransom demand resulting from a cyberattack by the first defendant,<sup>86</sup> into the second defendant's account with Bitfinex (a cryptocurrency exchange operated by the third and fourth defendants).<sup>87</sup> The claimant sued the defendants in unlawful means conspiracy, and sought a proprietary injunction in respect of the Bitcoin.<sup>88</sup>

A proprietary injunction is an interim injunction preventing the defendant from dealing with asset(s) over which the claimant is asserting that he has a proprietary right pending trial.

The injunction was granted,<sup>89</sup> and one of the crucial issues tackled in the judgment was whether cryptocurrencies constituted property that could be the subject of a proprietary injunction.<sup>90</sup> At this point, it is crucial to note that something that constitutes property in this sense does not necessarily mean it is property in another sense (e.g. a prima facie duty of non-interference on the rest of the world).

Bryan J held that cryptoassets constituted property for the purpose of a proprietary injunction, and there were two steps in his reasoning. First, something does not have to fall within the traditional categories of 'choses in possession' and 'choses in action' for it to be considered property.<sup>91</sup> Second, cryptoassets satisfy the four requirements in *National Provincial Bank v Ainsworth* (i.e. "[they are] definable, identifiable by third parties, capable in their nature of assumption by third parties, and having some degree of permanence").<sup>92</sup>

In relation to the first step in his reasoning, Bryan J agreed with the analysis in the UKJT's Legal Statement<sup>93</sup> that *Colonial Bank v Whinney*<sup>94</sup> does not mandate that something needs to be a chose in action or a chose in possession in the traditional sense before it can be

---

<sup>86</sup> *ibid*, [2]-[12].

<sup>87</sup> *ibid*, [14]-[15].

<sup>88</sup> *ibid*, [49].

<sup>89</sup> *AA* (n 85 above), [63].

<sup>90</sup> *ibid*, [61]-[63].

<sup>91</sup> *ibid*, [58].

<sup>92</sup> *ibid*, [59].

<sup>93</sup> UK Jurisdiction Taskforce, *Legal Statement on Cryptoassets and Smart Contracts* (2019).

<sup>94</sup> [1885] 30 Ch D 261.

admitted into the category of ‘property’.<sup>95</sup> For example, EU carbon emissions allowances and milk quotas are property but are neither a chose in action nor a chose in possession.<sup>96</sup>

In relation to the second step in his reasoning, Bryan J did not provide any direct reasoning as to why the four requirements in *Ainsworth* were met, but noted that such requirements were met for the reasons identified in the UKJT’s Legal Statement.<sup>97</sup> According to the Statement, cryptoassets are definable and identifiable by third parties as there is a public address.<sup>98</sup> As for permanence, cryptoassets seem to have as much permanence as other conventional financial assets, which “may only exist until they are (for example) “cancelled, redeemed, repaid or exercised”.<sup>99</sup> Finally, cryptoassets are capable of assumption by third parties as they are designed to be transferable between system participants.<sup>100</sup> Finally, as for stability (which was curiously not mentioned by Bryan J), the UKJT consider cryptoasset systems to be stable enough despite not always having absolute finality and immutability,<sup>101</sup> noting that “even conventional assets are at risk of deterioration, corruption, or loss”.<sup>102</sup>

He also noted that the same conclusion (that the four requirements were met) was reached in the Singaporean case of *B2C2 v Quoine*.<sup>103</sup>

At this point, it is important to note the misapplication of the *Ainsworth* criteria by the UKJT. Specifically, the *Ainsworth* criteria are intended to apply to rights and not things – in *Ainsworth* itself, the question was whether the *right* that the claimant had was capable of binding third parties, not whether a *thing* constituted property. Indeed, the *Ainsworth* criteria presuppose that there is a right – and it is this right that is being evaluated for whether it has

---

<sup>95</sup> *AA* (n 85 above), [58] (‘property’ in the sense of granting a proprietary injunction; see [61]).

<sup>96</sup> *ibid*, [58], quoting para 82 of the UKJT Legal Statement. Presumably, Bryan J would think that they too are ‘property’ for the purpose of granting a proprietary injunction.

<sup>97</sup> *ibid*, [59].

<sup>98</sup> UK Jurisdiction Taskforce (n 93 above), para 49.

<sup>99</sup> *ibid*, [52].

<sup>100</sup> *ibid*, [51].

<sup>101</sup> *ibid*, [53]-[57].

<sup>102</sup> *ibid*, [56].

<sup>103</sup> *B2C2 v Quoine* [2019] SGHC(I) 3 (“*Quoine* SGHC”). The *Quoine* litigation will be explored in Section 5.3 below.

third party effect. Thus, without knowing what the relevant right is in relation to a digital asset, it is conceptually impossible to properly apply the *Ainsworth* criteria. The criteria simply cannot be applied to a thing without knowing what the relevant right is. Judges in many other cases (including the ones explored below)<sup>104</sup> have made the same error – applying the *Ainsworth* criteria to cryptoassets (or certain type(s) of them), in reaching the conclusion that they are ‘property’ for the purposes of interim injunctions and insolvency, and can be held on trust.

Bryan J then explored the principles governing the grant of a proprietary injunction.<sup>105</sup> He noted that there must first be a serious issue to be tried, and if so, the court must consider whether the balance of convenience weighs in favour of granting the relief sought. In relation to the second element, one must consider the adequacy of damages in compensating the claimant, the adequacy of the cross-undertaking in damages, and the “overall balance of convenience” including the merits of the underlying claim.

Bryan J held that there was a serious issue to be tried. The claims were “very strong”<sup>106</sup> against the first and second defendants given that they appeared to be the ones who perpetrated the blackmail and extortion, and obtained the sums by ransom. As for the third and fourth defendants, they may have been “mixed up in another’s wrongdoing”<sup>107</sup> and had arguably come into possession of Bitcoin “in the furtherance of a fraud”.<sup>108</sup>

In turn, the balance of convenience lay firmly towards granting relief, and damages would not be an adequate remedy given that the Bitcoins could be dissipated and the claimant had a “strong claim”<sup>109</sup> to the Bitcoins.<sup>110</sup>

---

<sup>104</sup> Until the end of Section 5.3 below.

<sup>105</sup> *AA* (n 85 above), [62].

<sup>106</sup> *ibid.*, [63].

<sup>107</sup> *ibid.*, [64].

<sup>108</sup> *ibid.*, [64].

<sup>109</sup> *ibid.*, [65].

<sup>110</sup> *ibid.*, [65].

There are many other cases that follow a similar fact pattern, where there has been some kind of fraud or misappropriation or induced transfer and the claimant seeks a proprietary injunction, a freezing injunction, and/or various disclosure orders such as a Bankers Trust order.<sup>111</sup>

## 5.2 Insolvency cases

The second group of cases concern whether digital assets are ‘property’ for the purpose of insolvency. Some of these cases also discuss the issue of holding digital assets on trust (and I will not focus on the trust issue in detail here).

The New Zealand case of *Ruscoe v Cryptopia*<sup>112</sup> concerned the insolvency of the New Zealand cryptocurrency exchange Cryptopia. The main conceptual issues tackled in the judgment were whether cryptocurrencies constituted property for the purpose of insolvency,<sup>113</sup> and if so, whether they could be held on trust. The judgment also dealt with the issue of whether as a matter of fact the cryptocurrencies were held on trust by the exchange for the account holders.

In relation to the question of whether cryptocurrencies constituted property, Gendall J (1) applied the test in *Ainsworth* and held that the four elements were satisfied,<sup>114</sup> and (2) responded to some objections against recognising cryptocurrency as property.<sup>115</sup> As such, he held that cryptocurrencies constituted property for the purpose of insolvency.

---

<sup>111</sup> E.g. *Janesh s/o Rajkumar v Unknown Person* [2022] SGHC 264; *Fetch.ai v Persons Unknown* [2021] EWHC 2254 (Comm); *Osbourne v Persons Unknown* [2022] EWHC 1021; *CLM v CLN and Others* [2022] SGHC 46; *Ion Science v Persons Unknown* (unreported), 21 December 2020 (Commercial Court). I will not discuss these cases due to limitations of space and the issues being similar to those discussed.

<sup>112</sup> *Ruscoe v Cryptopia Ltd* [2020] NZHC 728.

<sup>113</sup> Under s.2 of the New Zealand Companies Act 1993; see *Cryptopia* (n 112 above), [46]. Also, if something is property under one meaning (e.g. insolvency), that does not necessarily mean that it is property under another meaning (e.g. non-interference rights).

<sup>114</sup> *Cryptopia* (n 112 above), [104]-[119].

<sup>115</sup> *ibid.*, [122]-[132].

In applying the *Ainsworth* test, Gendall J held that cryptoassets are definable in the sense that they can be isolated from other assets, because the “data allocated to one public key will not be confused with data allocated to another public key”.<sup>116</sup> Having distinct public keys where assets can exist allows cryptoassets to be distinguished from each other.<sup>117</sup> They are identifiable by third parties (in the sense that there is an owner that can be identified by third parties)<sup>118</sup> because the holder of private key has the power to exclude others from accessing the cryptoasset.<sup>119</sup> In turn, they are capable of assumption by third parties (in the sense that (1) “[t]hird parties must respect the rights of the owner in that property” and will be subject to legal consequences if they do not,<sup>120</sup> and that (2) the asset will normally potentially desirable to third parties),<sup>121</sup> because cryptocurrencies are capable of being the subject of dishonest dealing, and are actively traded in the markets.<sup>122</sup> Finally, they have some degree of permanence and stability. There is sufficient stability because the blockchain system records the history of a cryptoasset on a public record, and standard cryptocurrency systems do not allow for the “arbitrary cancellation of coins”.<sup>123</sup> As for permanence (which is a low threshold to satisfy), cryptocurrencies have sufficient permanence (given its features such as being publicly recorded on a stable ledger) if a ticket to football match (which can exist for a very short duration) has the necessary degree of permanence to be property, and if money in bank accounts (which can have a short life insofar as bank payments entail the replacement of one asset with another) have enough permanence to be property.<sup>124</sup>

Again, as with Bryan J in *AA*, Gendall J in *Cryptopia* has misapplied the *Ainsworth* criteria to things instead of rights, as he has applied the test to cryptocurrencies. The

---

<sup>116</sup> *ibid.*, [105].

<sup>117</sup> *ibid.*, [104]-[105]; also see [106]-[108].

<sup>118</sup> *ibid.*, [109].

<sup>119</sup> *ibid.*, [109]-[113].

<sup>120</sup> *ibid.*, [114].

<sup>121</sup> *ibid.*, [114].

<sup>122</sup> *ibid.*, [115]-[116].

<sup>123</sup> *ibid.*, [118].

<sup>124</sup> *ibid.*, [117]-[118].

awkwardness of conflating things and rights can also be seen in Gendall J’s application of the ‘capable of assumption by third parties’ criterion, because in saying that “[t]hird parties must respect the rights of the owner in that property”,<sup>125</sup> he simply assumed (without establishing) that there were rights to that property.

In addition, Gendall J used the *Ainsworth* criteria to conclude that cryptocurrencies are property in a different sense from *AA* – namely property for the purpose of insolvency instead of interim applications. The fact that the *Ainsworth* criteria are being misapplied to justify *different* conclusions can perpetuate the notion that they are legitimate criteria to apply in deciding whether digital assets are ‘property’ regardless of the purpose.

Gendall J also responded to the arguments that (1) cryptocurrency is mere information and thus cannot be property, (2) cryptocurrency cannot be property because it is neither a chose in possession nor a chose in action, and the potential objection that (3) cryptocurrency should not be recognised as property for public policy reasons.<sup>126</sup> In sum, he held that cryptocurrency is more than merely digitally recorded information because it cannot be double spent<sup>127</sup> (given the rules of the blockchain system), and that *Colonial Bank v Whinney*<sup>128</sup> on its proper interpretation does not pose an obstacle to recognising cryptocurrency as property.<sup>129</sup> He also held that the use of cryptocurrencies for the purposes of money laundering and criminal activity should not prevent them from being recognised as property, and that “honest commercial developments may well be hindered”<sup>130</sup> if cryptoassets were not to be recognised as property.<sup>131</sup>

As such, Gendall J held that cryptocurrencies constituted property for the purpose of insolvency, and were capable of being held on trust.<sup>132</sup>

---

<sup>125</sup> *ibid*, [114]; see n 120 above and text thereto.

<sup>126</sup> *ibid*, [122]-[132].

<sup>127</sup> *ibid*, [127]: “a cryptocoin can...be sold only once.”

<sup>128</sup> *Colonial Bank* (n 94 above).

<sup>129</sup> *Cryptopia* (n 112 above), [123]-[125].

<sup>130</sup> *ibid*, [130].

<sup>131</sup> *ibid*, [129]-[132].

<sup>132</sup> *ibid*, [133].

Similar issues were dealt with in the Hong Kong case of *Re Gatecoin Ltd*,<sup>133</sup> which concerned the insolvency of the Hong Kong cryptocurrency exchange Gatecoin. Like in *Cryptopia*, the Hong Kong Court of First Instance held that cryptocurrencies constituted property for the purpose of insolvency<sup>134</sup> and were capable of being held on trust. The court thought it was appropriate to apply the test in *Ainsworth* to determine whether cryptoassets were property for the purpose of insolvency,<sup>135</sup> and followed the analysis in *Cryptopia*.<sup>136</sup> In so doing, it misapplied the *Ainsworth* criteria to things (i.e. cryptoassets) and not rights.

### 5.3 Miscellaneous contract and trust cases

The third group of cases concern contractual and/or trusts issues outside the context of insolvency and outside the context of interim applications.

A case that has been the subject of considerable discussion<sup>137</sup> is the Singaporean case of *Quoine*.<sup>138</sup> The claimant was a market maker who was a user of the defendant's trading platform, and entered into BTC-ETH trades on the platform with various counterparties via algorithmic trading software that did not require any human intervention. An unintended loophole in the defendant's code caused trades to be executed at a rate which allowed B2C2 to be able to obtain BTC at approximately 250 times<sup>139</sup> below the market price.

The defendant's chief technology officer (CTO) reversed the trades on the basis that there was a mistake in the code, and the claimant claimed that the reversal of the trade was a

---

<sup>133</sup> [2023] HKCFI 914.

<sup>134</sup> Under s.197 of the Companies (Winding Up and Miscellaneous Provisions) Ordinance (Cap. 32, Laws of Hong Kong) and s.3 of the Interpretation and General Clauses Ordinance (Cap. 1, Laws of Hong Kong).

<sup>135</sup> *Gatecoin* (n 133 above), [59].

<sup>136</sup> *ibid*, [57]-[59].

<sup>137</sup> See e.g. Kelvin FK Low and Eliza Mik, 'Lost in Transmission: Unilateral Mistakes in Automated Contracts' (2020) 136 LQR 563; Vincent Ooi and Kian Peng Soh, 'Rethinking mistake in the age of algorithms: *Quoine Pte Ltd v B2C2 Ltd*' (2020) 31 KLJ 367; Low, 'Quoines in Cryptopia' (n 57 above).

<sup>138</sup> *Quoine v B2C2* [2020] SGCA(I) 2 ("*Quoine* SGCA"); appealed from *Quoine* SGHC (n 103 above).

<sup>139</sup> *Quoine* SGCA (n 138 above), [2].

breach of contract and a breach of trust. The defendant argued that there was no breach of contract or trust, and that there was a unilateral mistake, and was therefore entitled to reverse the trade.

It was held that the defendant was liable to the claimant for the reversal of the trades. The Singapore Court of Appeal majority affirmed the first instance judge's conclusion that there was no contractual term that entitled the defendant to reverse the trades.<sup>140</sup> However, since there was no trust over the cryptocurrencies there was no breach of trust (even assuming that BTC could be the subject-matter of a trust).<sup>141</sup> Furthermore, the defendant was not unjustly enriched, because the claimant received the relevant cryptocurrencies under valid and enforceable contracts and so there was no unjust factor.<sup>142</sup>

In relation to the defendant's unilateral mistake argument, the majority held that although the defendant had a mistaken belief that the relevant program was working normally, the claimant was not aware of the software loophole when the trades were entered into and thus did not know about the mistake at the time of contracting.<sup>143</sup> As such, the trades were not void or voidable for unilateral mistake.<sup>144</sup>

It is worth noting that the majority briefly referred to the four requirements in *Ainsworth* (and the first instance judge's discussion of it), as part of the issue of whether cryptocurrencies were capable of being the subject-matter of a trust. The majority noted that although the first instance judge concluded that the four requirements in *Ainsworth* were satisfied, he "left open the question of what the precise nature of the property right was, having been satisfied that cryptocurrency could be treated as property in a generic sense".<sup>145</sup> Indeed, the first instance judge did not provide much reasoning as to why cryptocurrencies met the four requirements in

---

<sup>140</sup> *ibid.*, [7], [59]-[77].

<sup>141</sup> *ibid.*, [7], [137]-[149].

<sup>142</sup> *ibid.*, [7], [130]-[136].

<sup>143</sup> *ibid.*, [125]-[126].

<sup>144</sup> *ibid.*, [128] and [80].

<sup>145</sup> *ibid.*, [138].

*Ainsworth*<sup>146</sup> – because the defendant did not dispute the point that they could be treated as property.<sup>147</sup>

Again, the first instance judge in *Quoine* has misapplied *Ainsworth* to things (cryptocurrencies) instead of rights, and this slippage was neither spotted by the majority<sup>148</sup> nor mentioned by the dissenting judge in the Court of Appeal.

Another relevant Singaporean case is *Ho Kai Xin*.<sup>149</sup> This case involved cryptocurrency payments from the claimant that were supposed to be directed by the defendant to the claimant’s employees, but were instead misappropriated by the defendant into various addresses controlled by herself.<sup>150</sup>

The claimant applied for summary judgment, seeking a declaration that the cryptocurrencies in the defendant’s addresses were held on constructive trust for the claimant.<sup>151</sup>

The court granted the claimant’s application and declared that the cryptocurrencies were held on constructive trust for the claimant. In reaching this conclusion, the court (once again) referred to *Ainsworth*<sup>152</sup> and held that cryptoassets are property,<sup>153</sup> and could thus form the subject-matter of a trust.<sup>154</sup> The court also accepted the evidence that the defendant fraudulently transferred the cryptocurrencies to herself,<sup>155</sup> and thus granted the constructive trust following *Westdeutsche*.<sup>156</sup>

---

<sup>146</sup> *Quoine* SGHC (n 103 above), [142], where it is only noted that cryptocurrencies have the “fundamental characteristic of intangible property as having a thing of value”.

<sup>147</sup> Property in a “generic sense”: *ibid*, [142].

<sup>148</sup> *Quoine* SGCA (n 138 above), [138] (noting that the first instance judge applies *Ainsworth*, but does not note the slippage).

<sup>149</sup> *ByBit Fintech Limited v Ho Kai Xin* [2023] SGHC 199.

<sup>150</sup> [2].

<sup>151</sup> [2] and [5].

<sup>152</sup> *ibid*, [33]; see also [31]-[32] for background reasoning.

<sup>153</sup> By virtue of meeting the requirements in *Ainsworth*: *ibid*, [33].

<sup>154</sup> *ibid*, [29]-[39].

<sup>155</sup> *ibid*, [41].

<sup>156</sup> *ibid*, [42]; citing *Westdeutsche Landesbank Girozentrale v Islington London Borough Council* [1996] 1 AC 669, 716.

As with the other cases discussed, the judge has misapplied *Ainsworth* to things (cryptoassets) and not rights. Here he has misapplied the *Ainsworth* test to justify the conclusion that cryptoassets are property for yet another purpose,<sup>157</sup> namely that they are capable of being held on trust.<sup>158</sup> Apart from creating the danger(s) mentioned earlier,<sup>159</sup> this misapplication of *Ainsworth* simply skips over the crucial question of what *right* is being held on trust – there is no discussion about the content of the right that is being held on trust.<sup>160</sup>

#### 5.4 Gap in the case law

None of the cases explored go into any detail about the substantive content of the property right, i.e. what package of non-interference rights the claimant has against the world in respect of the digital asset. Nor do they discuss how to acquire or transfer such a right, or the strength of this right as against third parties.

This leaves an obvious gap in the case law, and this thesis intends to address this issue that has been underexplored in the case law. Having no clarity about what the content of the property right is means that there will be no clarity on *what it is* that is being (e.g.) held on trust, transferred to another person, or subject to a charge.

Indeed, as stated earlier, establishing that the four requirements in *Ainsworth* are satisfied does not shed light on what the scope of the relevant non-interference rights are.<sup>161</sup> In fact, it does not even shed light on whether it is conceptually possible to have non-interference rights in respect of digital assets.

---

<sup>157</sup> Specifically a third purpose (capability of being held on trust; the first two purposes are interim applications and insolvency).

<sup>158</sup> *Ho* (n 149 above), [29]-[39].

<sup>159</sup> See Section 5.2, para 6 above (misapplying *Ainsworth* in different contexts; danger of perpetuating impression that *Ainsworth* criteria are legitimate criteria to apply for ascertaining whether something is ‘property’ generally).

<sup>160</sup> *Ho* (n 149 above), [31] – Jeyaretnam J mentions the ‘right’ attached to a cryptoasset but that is merely a reference to the transactional power and not the rights in relation to such a power.

<sup>161</sup> See Section 3.4 above.

The misapplication of the *Ainsworth* test to things instead of rights is an illegitimate shortcut that allows courts to conclude that digital assets constitute ‘property’ for various purposes (interim injunctions, insolvency, capability of being held on trust) – without considering what the content of the property right in fact is. If cases continue to apply the *Ainsworth* test in such manner, the question of what the content of the property right is may never be addressed in sufficient depth – it makes people simply assume digital assets are ‘property’ in a vague or general sense without considering the content of the property right, or even the conceptual capability of having such right(s).

Thus, the issue is not merely that the case law produces a ‘gap’ per se. It is that misapplying *Ainsworth* to things to conclude that digital assets are ‘property’ produces a band-aid solution in certain contexts (interim applications, insolvency, trusts, and potentially more), and actively obscures the fundamental questions by directing people’s focus away from them. This actively reduces the chance that the ‘gap’ in the case law will be adequately addressed.

In answering my four research questions, this thesis also reduces the likelihood that people will mistakenly apply the *Ainsworth* to digital assets (them being things), and thereby refocuses the attention on the crucial questions that need to be answered.

Indeed, if one has a reasonably clear answer to my four research questions, courts would feel less of a need to apply the *Ainsworth* test. If there is clarity as to (for example) the subject-matter and content of a property right to a digital asset, courts can directly answer the question of whether it is ‘property’ for the purpose of interim applications and insolvency, by reference to the features of the property right, without needing to resort to the *Ainsworth* criteria.

In this sense, the temptation to apply the *Ainsworth* test also arises precisely because there is no clarity as to the fundamental questions about (e.g.) the subject-matter and content of a property right to a digital asset, thus creating the need for a stopgap yardstick for assessing whether digital assets are ‘property’ for various purposes.

The following section will address my first research question. It will establish that it is conceptually possible to have a property right in respect of a digital asset, and that (on a fundamental level) it is normatively desirable to introduce a property right in respect of a digital asset.

## **6. Whether digital assets are conceptually capable of constituting property, and the normative case**

In order to answer the questions of how a property right in a digital asset is to be acquired or transferred, or explore its strength against third parties, it must first be established that digital assets are conceptually capable of being the object of a property right. It would also be useful to establish that a legal system that offers parties the possibility of having property rights in digital assets is normatively more valuable than one that does not offer parties that possibility.

These two issues will be explored in turn.

### **6.1 Features of digital assets in more detail**

To know whether a digital asset is conceptually capable of constituting the object of property rights, it would be useful to articulate the key features of a digital asset in more detail.

In Section 2 it was established that a digital asset consists of a power to execute transactions on a blockchain (or other distributed ledger).<sup>162</sup> It would be helpful to explore the key features of a digital asset (the transactional power) in more detail.

The transactional power carries three features:

---

<sup>162</sup> See also Fox (n 5 above).

- (1) it exists as a notional quantity unit, and is manifested through the combination of software operated by a network of participants, and data instantiated on a network;
- (2) it is rivalrous; and
- (3) it is independent of the legal system and other persons.

These are the three necessary ingredients of a ‘crypto-token’<sup>163</sup> according to the Law Commission, and of a ‘digital asset’ under the DIFC DAL.<sup>164</sup>

### ***6.1.1 Notional quantity unit + Data entries and software***

A digital asset exists as a notional quantity unit that is manifested through the “combination of the active operation of software by a network of participants and network-instantiated data”.<sup>165</sup>

It exists as a ‘notional quantity unit’, in the sense that all digital assets are denominated in numerical units (e.g. 2 Bitcoin, 3 Ether, etc).

Its existence is manifested via two features, without which there would be no digital asset. The first feature is the active operation of software by a network of participants. The core software rules of the blockchain nodes for example are necessary for the blockchain infrastructure to run, and such software needs to be actively operated by participants in the network in order for the blockchain to keep processing, verifying and adding transactions. Without this, there would be no blockchain or distributed ledger, and thus no digital asset.

The second feature is network-instantiated data. This means that the relevant data (the public address and private key, combined with the information about the number of ‘quantity

---

<sup>163</sup> The definition of a crypto-token in the Law Commission’s Final Report (n 36 above) only includes the first element (see page ix), but a crypto-token is also a ‘third category thing’ according to the Law Commission so also carries features 2 and 3: see Law Commission, *Final report* (n 36 above), 4.5, and 4.22-4.47.

<sup>164</sup> DAL Article 8.

<sup>165</sup> Law Commission, *Final report* (n 36 above), 4.45.

units' in a particular public address is instantiated (or recognised) as an object under the software rules of the blockchain network. When this happens, the data entries on the blockchain can be manipulated under certain conditions, because instantiation as an object confers functionalities in respect of the data, namely the power to sign transactions and messages using the private key, in relation to assets in the public address to which the private key is associated. Without instantiation on the network, the data would have no functionality, and there would be no digital asset.

Without these two features, a digital asset would simply not exist.

### **6.1.2 'Rivalrous'**

A digital asset is rivalrous<sup>166</sup> because the use of a digital asset (in terms of signing transactions on the blockchain) necessarily prejudices the use of the digital asset by another person. If one exercises a power that is attached to a digital asset, it becomes 'spent' and cannot be used by another person. Thus, if one exercises a power to transfer a digital asset (e.g. the one Bitcoin he has in his address) to another address, that power becomes 'spent' and the Bitcoin would no longer exist in his address. Similarly, if one exercises a power to vote (e.g. on a governance proposal) that is attached to a particular digital asset, that vote becomes 'spent'.<sup>167</sup>

This distinguishes a digital asset from 'mere data' or 'pure information'. Pure information, such as (e.g.) the fact that X has control of one Bitcoin in a particular address, is not rivalrous. If X tells Y that he has control of one Bitcoin in a particular address, *both* X and Y have the information. In contrast, if X executes a blockchain instruction and sends that Bitcoin to Y's address, X no longer has the Bitcoin.

---

<sup>166</sup> *ibid.*, 4.27-4.47.

<sup>167</sup> Unless the vote is programmed to be modifiable.

### **6.1.3 'Independent of the legal system and other persons'**

A digital asset is also independent of the legal system and other persons.<sup>168</sup>

It is independent of the legal system because even if one takes the legal system away, a digital asset would still exist, as the network of computers and software and physical infrastructure that are required for the digital asset to exist would remain intact. This contrasts with debts, which are dependent on a legal system. Without a legal system that recognises contracts, a debt would not exist. A digital asset also contrasts with some Hohfeldian liberties such as carbon trading allowances, because these liberties function only within the backdrop of an underlying rule that prohibits particular behaviour (in this case legislation or regulations that limit the amount of carbon dioxide one is allowed to emit).<sup>169</sup> Such a rule is created by the legal system, and thus carbon trading allowances (and other types of Hohfeldian liberties that exist within the backdrop of a prohibitive legislative rule) are dependent on the legal system.

A digital asset is also independent of persons. As long as the underlying computers and infrastructure exists, the digital asset exists. This contrasts with a debt, which requires two people (the creditor and the debtor).

### **6.1.4 Digital assets as physical assets?**

It has been established that a digital asset consists of a factual power to make transactions on the blockchain, and contains the three features that have just been discussed.

---

<sup>168</sup> Law Commission, *Final report* (n 36 above), 4.22-4.26.

<sup>169</sup> See e.g. *Armstrong v Winnington* [2012] EWHC 10 (Ch), [2013] Ch 156, at [7]-[8].

Nonetheless, one may ask the following question: if a digital asset is manifested by the active operation of software by a network of participants,<sup>170</sup> and software runs on computers, then can we say that the digital asset is just the physical areas on the computers in which the entries containing transactions involving the digital asset are stored?

It is suggested that this is not the case, as a digital asset is, fundamentally, not any of the underlying physical assets that are necessary for it to exist. Indeed, many physical assets (such as computers and cables) need to exist in order for a digital asset to exist, but they do not form part of the digital asset itself.

Take Bitcoin as an example. If:

1. one of the individual computers that store a copy of the Bitcoin blockchain gets destroyed; and
2. a Bitcoin consisted of all the physical areas on each computer in which the entries involving that Bitcoin<sup>171</sup> are stored, then
3. destroying one computer would necessarily mean that the Bitcoin would be damaged, since part of the asset would necessarily be damaged.

However, in reality, even if one of the computers gets destroyed, the Bitcoin would remain completely intact as the remaining computers would still be able to process and validate transactions on the network.

In contrast, if a physical asset is ‘my house’, damaging *any* of the bricks that make up my house would necessarily mean that my house has been damaged. If something is a physical

---

<sup>170</sup> Plus network-instantiated data, which is really just the functionalities of the data under the relevant *software* rules.

<sup>171</sup> Specifically, the areas containing the electrons and associated voltage levels that represent the binary 1s and 0s that in turn represent the entries involving that Bitcoin.

asset, damaging any of the physical parts that constitute the asset would mean there is damage to the asset. In contrast, if such parts are damaged but the asset remains undamaged, this means that the asset is not a physical one.

A digital asset is ultimately an abstract asset,<sup>172</sup> as opposed to anything physical or tangible. It *requires* the existence of the underlying physical infrastructure and equipment, but it would be a mistake to assume that such infrastructure and equipment forms *part* of the digital asset. If this were the case, then damage to the underlying infrastructure would necessarily mean that the digital asset would be damaged, and this is clearly not the case.

Indeed, as noted by the Law Commission, the digital asset is ideational.<sup>173</sup> It is not physical.

## 6.2 Conceptual capability of constituting property

Having clarified the key features of a digital asset in more detail, it would now be appropriate to explore whether it is conceptually possible to have property rights in respect of digital assets.

If there are claim rights against the world not to interfere with a particular object or thing (or the use of a such a thing) under certain conditions, this means that there are corresponding duties owed by the rest of the world to the right-holder in respect of that object or thing.<sup>174</sup>

Conceptually speaking, it is possible for such rights to exist in respect of a digital asset, just as it is possible to have such rights in respect of a physical asset. For example, the right to

---

<sup>172</sup> Fox (n 5 above), 3: “a digital asset is an ideational thing”.

<sup>173</sup> Law Commission, *Final report* (n 36 above), 4.18.

<sup>174</sup> These can be duties not to interfere with the thing itself, or impair its use or usability – the scope of the non-interference duties can be different. For example, the non-interference duties in respect of land are more extensive than those in respect of chattels (since nuisance encompasses a right not to impair the usability of the land (Donal Nolan, ‘The Essence of Private Nuisance’ in Ben McFarlane and Sinead Agnew (eds), *Modern Studies in Property Law, Volume 10* (Hart Publishing, 2019) 71) whereas in relation to chattels the duty is to not make physical contact with or physical damage to the thing itself (whether intentionally or negligently), or intentionally cause a total impairment of use of the thing (see Simon Douglas, ‘Actionable Interferences in the Chattel Torts: A New Perspective on Economic Loss’ in Simone Degeling, James Edelman, James Goudkamp (eds), *Torts in Commercial Law* (Routledge, 2011) 87, 88-104).

sue in conversion, trespass, and negligence (in respect of chattels), as well as the right to sue in trespass,<sup>175</sup> nuisance, and negligence (in respect of land), involve the rest of the world being under a duty not to physically interfere with the asset<sup>176</sup> or impair its use (under specific conditions).<sup>177</sup>

Like a physical asset, a digital asset is also a rivalrous object that is independent of the legal system, so there can be a conceptually similar structure of rights that can be imposed. It is possible to have claim-rights that correspond with duties on the rest of the world not to interfere with the use of a digital asset, i.e. duties not to interfere with someone's ability to exercise their transactional power(s).<sup>178</sup> It is also possible to have duties not to interfere with someone's digital asset itself – i.e. duties not to diminish the transactional capabilities of the digital asset itself.<sup>179</sup>

In both the physical and digital asset contexts, the duties<sup>180</sup> are targeted at the specific (rivalrous) object that is independent of the legal system and persons. If the dut(ies) are infringed, the claimant can sue. There are, of course, questions as to what the precise content of the duties can (and should) be, which will be examined in more detail in a later section.<sup>181</sup> The key point here is that it is conceptually possible for the law to recognise some form of 'non-interference rights' in respect of a digital asset.

---

<sup>175</sup> Trespass to land.

<sup>176</sup> Ben McFarlane and Simon Douglas, 'Property, Analogy and Variety' (2022) 42 OJLS 161, 164-165.

<sup>177</sup> Douglas (n 174 above), 95-96; *Burroughes v Bayne* (1860) 5 H & N 296 (chattels). In relation to land, the duty is also breached where there is no impairment of actual use, since it involves a duty not to impair the *usability* of the land: Nolan (n 174 above), 74.

<sup>178</sup> This duty can be triggered when specific conditions are met, see e.g. DAL Article 14(2)(d) (loss) and 14(2)(c) (intention or recklessness).

<sup>179</sup> This would not cover (e.g.) a DDoS attack because that involves diminishing C's ability to exercise the transactional powers/capabilities associated with the asset (e.g. the power to transfer), but does not diminish the transactional powers/capabilities associated with the asset (as the power to transfer still exists).

<sup>180</sup> No matter whether they are duties of 'non-interference with the thing' or 'non-interference with the use of the thing'.

<sup>181</sup> See Section 6.2.2 below (and in particular Sections 6.2.2.1-6.2.2.5).

Non-interference rights in respect of a digital asset have practical utility, most crucially because digital assets can be involuntarily alienated or destroyed.<sup>182</sup> Thus, such rights would protect against (at least) several ‘core situations’ where the duty is infringed, such as intentional<sup>183</sup> misappropriation, freezing,<sup>184</sup> or burning<sup>185</sup> of a digital asset. All of these actions involve diminishing or eliminating the number of transactional functionalities over the digital asset that the claimant can exercise using his private key.

Depending on the precise boundaries of the duty, it may also protect against various situations where a defendant (D) prevents someone (C) from exercising positive control over a digital asset (or severely impedes his ability to do so) without diminishing the number of transactional functionalities C can exercise in respect of the digital asset using the private key. An example would be where there is a distributed denial of service (DDoS) attack on the relevant application that C uses to access the functionalities of a digital asset, which makes C unable to access his private key for a certain period of time and thus unable to make transactions in respect of the digital asset.<sup>186</sup>

In such a situation, there is no diminution in the number of functionalities that can be exercised over the digital asset using the private key,<sup>187</sup> but there is a denial of access that prevents him from being able to use his digital asset. This contrasts with the situation where he

---

<sup>182</sup> See e.g. Law Commission, *Final report* (n 36 above), 9.70: crypto-tokens are “susceptible to involuntary alienation” and “vulnerable to interference, deprivation and misappropriation”.

<sup>183</sup> By ‘intentional’ I am not referring to intending the relevant act per se (e.g. the act of burning), but intending the act with the knowledge or belief that someone else has a better title to the asset, or at least without mistakenly believing that he himself owns the asset. Under DAL Article 14(1)(c)(i), an impairment is not ‘intentional’ unless he “knows that another person (B) has an interest in the Digital Asset”.

<sup>184</sup> Freezing involves disabling someone from being able to enter transactions on the blockchain in respect of the digital asset, or at a minimum, disabling someone from transferring the digital asset to another address. When a digital asset is frozen, it can often be ‘unfrozen’ with the effect that the ability to enter transactions in respect of the digital asset can be restored.

<sup>185</sup> A token is burnt if it is destroyed, or if it is transferred to a ‘burn address’ (an address with no private key). Where an asset is transferred to a burn address, no one can have control of the digital asset anymore, and no one can enter any transactions in respect of the digital asset. The digital asset is rendered obsolete, even though it technically ‘remains’ in the burn address.

<sup>186</sup> For more examples, see Liu, ‘Interference torts’ (n 36 above), section 5.1.

<sup>187</sup> Given that he still has the private key, and there is no change in the transactional functionalities that he can exercise in relation to the digital asset using his private key.

cannot exercise any of the transactional functionalities of the digital asset using his private key, such as (for example) where the digital asset has been misappropriated from the address.<sup>188</sup>

### ***6.2.1 Some differences from other types of rights***

Also, it is crucial to distinguish between non-interference rights in respect of a particular rivalrous object independent of the legal system (such as a digital asset or a chattel), and an exclusive right to ‘pure information’. In the digital asset context, non-interference rights effective against the world do not involve the latter.

This distinction seems to have been overlooked by Stevens, as he draws an analogy between (1) someone guessing the private key to a digital asset and then selling the digital asset, and (2) someone independently discovering where a pot of gold is buried.<sup>189</sup> He argues that because there is no claim in relation to (2) (given that the law does not confer exclusive rights to information, or exclusive rights to prevent others from using information),<sup>190</sup> there should not be a claim in relation to (1).

This analogy overlooks the distinction between a right to information that is effective against the world, and non-interference rights in relation to a rivalrous object (such as a digital asset) that are effective against the world. The effect of the former is that other people cannot use the relevant information (including (1) or (2)) even if they independently discover it. In contrast, with the latter, even if such information is discovered, there is generally no liability

---

<sup>188</sup> This situation gives rise to liability under Article 14 of the DAL. Misappropriating a digital asset leads to a complete impairment of use (satisfying the conduct requirement of ‘impairment’ in 14(2)(b)), causes loss (satisfying the ‘loss’ requirement in 14(2)(d)), and satisfies the mental requirement of ‘intentional or reckless’ in 14(2)(d) is also satisfied.

<sup>189</sup> Stevens (n 34 above), 623, 617.

<sup>190</sup> *ibid*, 617, 619-620. Nonetheless, he mentions statutory exceptions in the intellectual property context: see 619-620.

where the claimant's rivalrous object has not been interfered with and its use has not been impaired.<sup>191</sup>

The former is much more onerous, because (as mentioned) pure information is not rivalrous. It can exist in multiple locations, can be discovered, and is infinitely transmissible. Thus, if duties are imposed on defendants not to discover,<sup>192</sup> use, or disclose valuable information, this would be much more restrictive than a duty not to interfere with someone's use of a digital asset, which can only exist in one 'virtual location' (address) at any given time.

The proper analogue to discovering where a pot of gold is buried<sup>193</sup> is, rather, discovering someone's private key. In such a case there is no interference with the claimant's ability to exercise his transactional power, as the claimant can still exercise his transactional power given he *also* has the private key and the asset is still in the address. Thus, the scope of an exclusive right to information is fundamentally different from the scope of a right to non-interference in respect of a digital asset.

In contrast, if the defendant sells the digital asset by changing control of the digital asset to someone else,<sup>194</sup> this would indeed involve an interference with the claimant's ability to exercise the transactional power associated with the digital asset.<sup>195</sup>

Clarifying that introducing non-interference rights effective against the world in relation to a digital asset does not require the recognition of a general exclusive right to information is critical, because it directly feeds into the question of whether it is desirable to

---

<sup>191</sup> See nn 174-177 above and text thereto. I say 'generally' because in the context of land, there is also liability where the *usability* of the land has been interfered with. Nonetheless, digital assets are more analogous to chattels than to land as they can be 'moved' from space to space (address to address), as opposed to being immovable as in the case of land.

<sup>192</sup> Stevens discusses the discovery of information: Stevens (n 34 above), 617, 623.

<sup>193</sup> *ibid*, 617, 623.

<sup>194</sup> The prevailing opinion is that a transfer of title to a digital asset requires a 'change of control' (with the requisite intention to transfer title): see Law Commission, *Final report* (n 36 above), 6.39-6.42; DAL Article 12(1); Hin Liu, 'Transferring legal title to a digital asset' (2023) 5 JIBFL 317; Hin Liu, 'Transferring legal title to a digital asset: shared and limited control arrangements (Part 2)' (2024) 4 JIBFL 251.

<sup>195</sup> The claimant can no longer exercise the transactional power as he no longer has the private key to the address at which the digital asset is located.

introduce such non-interference rights. It is a less onerous right, and thus becomes easier to justify.<sup>196</sup>

Also, non-interference rights in the digital asset context do not need to impose strict liability duties on the defendant,<sup>197</sup> in contrast with the chattel torts (which do impose strict liability).<sup>198</sup> The duty not to interfere with someone's ability to exercise their transactional power could, for example, be breached only where a relatively strict mental requirement is satisfied (e.g. recklessness or intention, as adopted by Article 14 of the DIFC DAL).<sup>199</sup> As will be explored in Chapter 4, the information costs associated with physical and digital assets are different, which justifies a different scope of liability.

Furthermore, another difference between the physical and digital asset contexts is that in relation to the latter, there is no direct equivalent of a physical interference (given that a digital asset does not have molecular boundaries, and behaves in drastically different ways).<sup>200</sup> Thus, applying concepts such as 'physical interference' to digital assets gives rise to a whole host of problems.<sup>201</sup>

Indeed, this demonstrates that one must be vigilant to false parallels with existing types of assets such as information and physical assets, and distinguish the underlying concerns that apply to each type of asset. Obviously, the same is true for debts – most importantly, the fact that digital assets can be involuntarily alienated also makes the underlying concerns different from debts as a default. With debts, they cannot be involuntarily alienated.<sup>202</sup>

---

<sup>196</sup> See text to n 281 below.

<sup>197</sup> See e.g. Law Commission, *Final report* (n 36 above), 9.73. It is also recommending that the courts develop "specific and discrete principles of tortious liability" instead of directly applying the chattel torts to digital assets: see 9.76 and 9.83.

<sup>198</sup> See e.g. Liu, 'Interference torts' (n 36 above), section 4. Of course, there are other duties in relation to physical assets (outside of the chattel torts) that are not of strict liability (as is the case with the tort of negligence as regards property damage).

<sup>199</sup> DAL, Article 14(2)(c) and 14(1)(b)-(c).

<sup>200</sup> See Chapter 4, Sections 3.4 and 3.4.1.

<sup>201</sup> See Chapter 4, Section 3.4.1.

<sup>202</sup> See e.g. Law Commission, *Final report* (n 36 above), 3.54.

If D owes C £10, C's debt claim cannot suddenly be 'taken' by a third party. In order to transfer the debt to another person, this requires the actual or apparent authority of (or ratification by) C.<sup>203</sup>

Even in the case that there has been some kind of interference with one's ability to settle a debt (e.g. in the case of *OBG v Allan*),<sup>204</sup> the debt claim remains, as the creditor has given no actual or apparent authority to discharge the debt, and has not given any ratification.<sup>205</sup> In *OBG*, this was the case, as the defendants were invalidly appointed receivers who purportedly 'settled' certain contractual claims on behalf of the claimant company, but the debt claims remained extant (despite the claimant factually suffering economic losses). There is no 'involuntary alienation' of the debt as that is not possible.

In such a case, the law does not need to confer an extra remedy, as the debt claim still exists (which the claimant can sue on) and there are default remedies in the economic torts which may be available.<sup>206</sup>

In contrast, the fact that a digital asset can be involuntarily alienated *prima facie* means that if someone's use of their digital asset is to be protected, the law needs to actively step in to provide a solution in the form of non-interference rights.

This is because if a digital asset is involuntarily transferred to another address, he no longer has use of it, and needs a remedy if he wants to recover control of it (or recover its monetary value).<sup>207</sup> There is no right by default that a person can rely on. Such a situation does

---

<sup>203</sup> *Crantrave Ltd v Lloyds Bank plc* [2000] QB 917 (authority or ratification required for discharge of debt; see also Hugh Beale, *Chitty on Contracts: Volume 1 (General Principles)* (35<sup>th</sup> ed, Sweet & Maxwell 2023), 21-019 (fn98)). Under ordinary principles of agency law, the same should apply where there is a transfer of the debt (via an assignment or novation) instead of a discharge.

<sup>204</sup> [2007] UKHL 21.

<sup>205</sup> *Crantrave* (n 203 above).

<sup>206</sup> Douglas and McFarlane (n 32 above), 238-239.

<sup>207</sup> Some cases of involuntary alienation do attract remedies under existing law (e.g. a constructive trust where there is misappropriation: see *Ho* (n 149 above)). However, many situations do not (e.g. exercising a smart contract burn function), and in such situations, a remedy is needed. See Chapter 4, Section 2.3 for discussion of the gap in protection in respect of burning.

not happen in relation to debts, because a debt cannot be involuntarily alienated<sup>208</sup> – the creditor can still sue on it (and thus still has rights).

Although the underlying considerations and concerns are different when determining the interference regime for every type of asset, it is crucial to recognise that with each type of asset, the core aim is to provide an interference regime that provides the ideal balance between offering adequate protection to claimants and not overly stifling the liberty of potential defendants.

### ***6.2.2 Potential content of the property right***

Given this, it would be helpful to explore some of the potential positions in relation to the content of the property right. The previous discussion covered this in brief (e.g. in relation to how we can deviate from strict liability, and how the right could encompass denials of access via a DDoS attack). However, it would be helpful to provide more clarity as to the range of potential positions one can take in relation to the non-interference right.

Indeed, it is important to clarify some of the potential positions one can take in relation to the content of the property right. Specifically, the analytical distinctions between these positions need to be illuminated in order to ascertain what the appropriate content of the property right should be, and thereby provide enough protection for right-holders while not unduly stifling the liberty of third parties. The position adopted carries practical consequences and is not just a theoretical issue, because it directly determines the scope of protection available to the holder of a property right.

There are in theory an infinite number of positions one can take in relation to the content of the non-interference right. There is not much literature on the potential content of the

---

<sup>208</sup> Law Commission, *Final report* (n 36 above), 3.54.

property right in the digital asset context, and much of the discussion below will draw on the literature on physical assets. Five positions that have been mentioned in the academic literature and/or the law (mainly from the physical asset context, save (4)) will be explored. These can act as potential reference points to frame the relevant discussion, including in relation to whether they are feasible positions to adopt in the digital asset context, or contain elements that one can draw from in formulating the relevant non-interference regime for digital assets.

The five positions are as follows. First, there could be a right that others not interfere with the asset. Second, there could be a right to exclusive control of the asset. Third, there could be a right to exclude others from the “use, occupancy and possession’ of the asset. Fourth, there could be a right that others not impair the (actual) use<sup>209</sup> of the asset, with a mental requirement of intention or recklessness. Fifth, there could be a right that others not impair the usability of the asset.

The terms ‘right to exclude’ and ‘right of exclusion’ have been used to refer to any of the first three positions.

The five positions will be explored in turn.

#### 6.2.2.1 Position 1: Right that others not interfere with a thing

The first position is a right that others not (deliberately<sup>210</sup> or carelessly) interfere with a thing, and this is discussed by McFarlane and Douglas in the physical asset context.<sup>211</sup> Specifically, this position involves a duty not to physically interfere with a chattel or a piece of land – and

---

<sup>209</sup> I.e. ability to use.

<sup>210</sup> The act of interference must be deliberate, but there is no requirement that the defendant must know or believe that someone else has title to the thing (and thus can be liable even if he mistakenly believes that he owns the thing).

<sup>211</sup> McFarlane and Douglas (n 32 above), 164-166.

such a duty is what is being invoked when someone says he has a ‘right to exclude’ in relation to the thing.<sup>212</sup>

Likewise, Merrill and Smith note that “the identification of a thing as property communicates to perfect strangers that they have a duty not to take, intrude upon, or otherwise interfere with the thing”.<sup>213</sup> This duty corresponds with a right to non-interference with the thing.

A right to non-interference with a physical thing imposes duties on the rest of the world to ‘keep off’ that thing, e.g. a duty not to physically damage or make physical contact with a computer.<sup>214</sup> This does not involve a duty on the rest of the world not to impair the *use* of the thing, i.e. it would not include a duty not to make a computer slower in accessing certain websites or servers, in the absence of physical damage or contact with the computer.

This position is what McFarlane and Douglas believe the current English law position is in relation to the non-interference duties in respect of chattels and land. In other words, it is the package of rights<sup>215</sup> that a person with title has against the world in relation to the physical asset.<sup>216</sup>

The question then arises as to whether this position provides useful guidance in the digital asset context. Indeed, McFarlane and Douglas are referring to *physical* things, but it is suggested that a digital asset has certain similarities to physical things (e.g. independence from the legal system and other persons, rivalrousness, and susceptibility to involuntary alienation) that allow this position to offer a *prima facie* point of comparison.

---

<sup>212</sup> *ibid*, 164-166.

<sup>213</sup> Merrill and Smith (n 39 above), 140-141.

<sup>214</sup> (deliberately or carelessly).

<sup>215</sup> I.e. claim-rights (and not powers).

<sup>216</sup> McFarlane and Douglas (n 32 above), 164-166. Note, however, that Douglas in an earlier piece argues that a “complete impairment of use” is sufficient for liability in conversion even though there is no physical contact or damage to the property: see Douglas (n 174 above), 95-96. Also, Nolan criticises the ‘physical interference’ position as regards land: see Nolan (n 174 above), 80-85.

However, as will be explored in Chapter 4, the notion of an interference with a physical thing cannot be straightforwardly applied in the digital asset context, given the differences in the nature of physical and digital assets.<sup>217</sup>

For example, digital assets have no physical boundaries and are governed by the rules of code instead of the physical laws (of e.g. gravity and friction). There is therefore no direct analogy between physical and digital assets, and it is therefore not easy (or perhaps not possible) to ascertain the equivalent threshold for ‘interference with a digital asset’.<sup>218</sup> This uncertainty makes it more difficult for third parties to know what conduct gives rise to liability, and thus makes it more difficult to justify such an ‘equivalent’ duty.

This meaning, therefore, can only act as a very general reference point instead of offering granular guidance on the appropriate scope of liability in respect of digital assets.

#### 6.2.2.2 Position 2: Right to exclusive control

The second position is a right to exclusive control of a physical asset.

Penner refers to this as a “right to immediate exclusive possession of tangible property”,<sup>219</sup> and this encompasses not only a right not to have one’s tangible property interfered with, but also a right not to be dispossessed or deprived of control of such property (even if the defendant has not taken or damaged the property himself).<sup>220</sup> He also calls this a “right to exclude”<sup>221</sup> and a “right of exclusion”.<sup>222</sup>

---

<sup>217</sup> Chapter 4, Section 3.4.

<sup>218</sup> Chapter 4, Section 3.4.1.

<sup>219</sup> Penner (n 46 above) 139, 16.

<sup>220</sup> *ibid*, 156.

<sup>221</sup> *ibid*, 139, 26.

<sup>222</sup> *ibid*, 156.

Thus, the duties go beyond non-interference with the thing, and encompass certain duties not to completely impair someone's use of a thing, by depriving him of control or possession of it (despite no physical contact with or damage to the thing).

Insofar as this position encompasses the duties in Position 1, it encounters the same problems mentioned above in terms of how it is unable to offer guidance at a granular level in terms of determining the scope of liability in respect of digital assets.

However, the idea of deprivation of control is relevant because this is a situation that is worth addressing in order to protect people's use of their digital assets. As will be explored in Chapter 4, the proposed 'recovery of control' remedy allows one who has been deprived of control of a digital asset (or has otherwise lost control of it) to recover control of it.<sup>223</sup> Similarly, under the proposed impairment tort, there would be liability for depriving someone of control of a digital asset or totally impairing his use of it if the mental requirements are satisfied.<sup>224</sup>

### 6.2.2.3 Position 3: Right to exclude others from use, occupancy and possession

The third position is a right to exclude others from the "use, occupancy, and possession"<sup>225</sup> of a resource (Waldron).<sup>226</sup> The correlative duty here is more extensive than the previous position, because a defendant cannot use an asset even if the claimant has not been deprived of possession.<sup>227</sup>

---

<sup>223</sup> This remedy allows the claimant to recover control of a digital asset even if the defendant has not committed a wrong.

<sup>224</sup> See Chapter 4, Sections 4.1.1 (the conduct requirement) and 4.1.2 (the mental requirement).

<sup>225</sup> Jeremy Waldron, 'Property, Justification and Need' (1993) *Can J L & Jurisprudence* 185, 195.

<sup>226</sup> *ibid.*, 194-195.

<sup>227</sup> Waldron discusses this in the context of ownership, and the right to exclude ('R2') is only one of three rights that constitute ownership ('R1'-'R3'). Here, I focus on R2, but the three rights of ownership are the right to use (R1), the right to exclude (R2), and the power to transfer (R3). It is worth noting that right to use (R1) is not a right (but rather a liberty), and the power to transfer (R3) is a power instead of a right. R2 is the only claim right.

This position is very similar to what Merrill and Smith describe as a “right to exclude”.<sup>228</sup> According to Merrill and Smith, if someone has a right to exclude, others need to obtain the permission of such a person to “use, enter, exploit, or develop the thing”.<sup>229</sup> Such a person can “deny, grant, or condition access to the thing in such a way as to determine how it will be used”.<sup>230</sup>

This position can be applied to the digital asset context insofar as there can be duties on the rest of the world not to use the digital asset and not to exercise control over it.

#### 6.2.2.4 Position 4: Right that others not impair use of asset intentionally or recklessly, plus right to recover control of asset

The fourth position involves two rights. First, it involves a right that others not impair the right-holder’s (present or future) use<sup>231</sup> of an asset, intentionally or recklessly.<sup>232</sup> Second, it involves a right to recover control of an asset from someone who is currently in control of it but has no title to or a title that is inferior to that of the claimant.

This is the position adopted in Articles 14 and 15 of the DIFC DAL respectively, as will be explored in Chapter 4.<sup>233</sup>

This position is extremely relevant as it directly concerns the scope of the non-interference right in respect of a digital asset. The interference regime proposed in Chapter 4 will be very similar to that in Articles 14 and 15.<sup>234</sup>

---

<sup>228</sup> Merrill and Smith (n 39 above), 141.

<sup>229</sup> *ibid*, 141.

<sup>230</sup> *ibid*, 141.

<sup>231</sup> ‘Use’ i.e. ability to use.

<sup>232</sup> DAL, Article 14(1)(c) (intention) and 14(1)(b) (recklessness). Note that ‘intention’ here is a much more pro-defendant requirement than the ‘deliberate’ interference requirement under Position 1, as it requires (*inter alia*) the defendant to have knowledge that he does not have the best title to the asset.

<sup>233</sup> See Chapter 4, Sections 4.1 and 4.2 below.

<sup>234</sup> See Chapter 4, Sections 4.1 and 4.2 below.

This position does not require an interference with the thing (unlike position 1). For example, one can impair someone's ability to use the asset without interfering with an asset (e.g. if there is a DDoS attack that prevents someone from being able to access their digital asset, but the digital asset itself in terms of its transactional functionalities have not been affected). It also contains a mental element for impairments (unlike positions 2 and 3).<sup>235</sup> Furthermore, the impairment tort requires interference with a person's actual ability to use an asset (and not just its usability, as in position 5, explored below).

#### 6.2.2.5 Position 5: Right that others not impair usability of asset

The fifth position is a right that others not impair the right-holder's usability of an asset. This is the position adopted in the private nuisance context, where there is a duty not to unreasonably interfere with the use and enjoyment of land.<sup>236</sup> Nolan interprets this as a duty not to interfere with the usability of the land (which goes beyond a duty not to interfere with the actual use of the land).<sup>237</sup> Indeed, he notes that "private nuisance is not concerned with whether the *claimant* can use or enjoy her land at all, but only with whether (and to what extent) her *land* is capable of being used and enjoyed".<sup>238</sup>

The following example illustrates how an impairment of usability can happen without an actual impairment of use of the relevant asset. Suppose an owner of a piece of land is currently halfway across the world (and will continue to be abroad for two months). Disproportionately foul smells are emitted from a neighbour for 12 hours, in a way where a reasonable person's enjoyment of the land would have been significantly impaired if he were

---

<sup>235</sup> Position 1 requires a deliberate or careless interference.

<sup>236</sup> See e.g. James Goudkamp and Donal Nolan, *Winfield and Jolowicz on Tort* (20<sup>th</sup> ed, Sweet & Maxwell 2020), 15-010; *Read v Lyons & Co Ltd* [1945] KB 216, 236; *Newcastle-under-Lyme Corp v Wolstanton Ltd* [1947] Ch. 92, 107; Nolan (n 174 above), 71, 72, and 74.

<sup>237</sup> Nolan (n 174 above), 71, 73-75.

<sup>238</sup> *ibid*, 74.

on the land at the time. Here, there is a claim in nuisance, even though the owner's actual use of the land has not been affected or impaired (given that he is abroad and is not using the land, and cannot possibly return to the land in 12 hours), and will not be affected since he will be abroad for two months. Nonetheless, the usability of the land has been affected – given that the foul smells mean that the *land* is not capable of being used and enjoyed to the same extent.<sup>239</sup>

In the digital asset context, it is suggested that this meaning may be less appropriate because the non-interference rights are targeted at protecting the claimant's actual use of the asset.<sup>240</sup>

#### 6.2.2.6 Taking stock

As mentioned,<sup>241</sup> the fundamental aim of exploring the content of the non-interference right is to ascertain the appropriate threshold that strikes the best balance between (1) the holders of such a right and (2) the rest of the world, such that the former would be adequately protected and the liberty of the latter would not be unduly stifled.

Although the law is not wedded to any of the physical asset thresholds when considering what the scope of the non-interference right in respect of digital assets should be (given that the underlying considerations in relation to the two types of assets are different), analogies at the abstract level can be drawn where appropriate. Adaptations and relevant distinctions can then be made to cater for the digital asset context. These analogies and distinctions would be made at the 'substance' and the 'technique' levels.

As will be made clear from Chapter 4, the suggested scope of the right in respect of digital assets consists of most elements from position 4 (reflected in the impairment tort) as

---

<sup>239</sup> *ibid*, 74: "private nuisance is not concerned with whether the *claimant* can use or enjoy her land at all, but only with whether (and to what extent) her *land* is capable of being used and enjoyed" (emphasis added).

<sup>240</sup> I.e. actual ability to use the asset: see Section 6.3.1 below.

<sup>241</sup> See Section 6.2.1 above.

well as elements from position 2 (reflected in the recovery of control remedy).<sup>242</sup> Chapter 4 will also discuss why positions 1 and 5 will not be adopted in the digital asset context.

### 6.3 The normative case

Having discussed what a digital asset is, and how it is conceptually possible to have a property right in respect of a digital asset, the next question to explore is whether from a normative policy standpoint the law should recognise a property right in respect of digital assets.

It is not the case that something conceptually capable of being the subject of property rights is necessarily recognised as property. For example, human corpses are physical objects that can (conceptually) be the subject-matter of property rights (given that e.g. they exist in a distinct physical location and are visible), but prior to the 20<sup>th</sup> century they were not recognised as property,<sup>243</sup> for public policy reasons.<sup>244</sup> At that time, the law had made the decision that it was normatively undesirable to recognise human corpses as objects of property, but this was *despite* the fact that human corpses are conceptually capable of constituting objects of property.

Are there convincing normative reasons to confer property rights in respect of digital assets?

#### 6.3.1 The basic argument: giving effect to expectations

---

<sup>242</sup> It also reflects elements of Position 3 insofar as it imposes duties (in certain circumstances) on people not to (e.g.) use a digital asset (by exercising the transactional power(s) associated with the digital asset).

<sup>243</sup> See e.g. *R v Sharpe* (1857) Dears & B 160, 163; *Williams v Williams* [1882] 20 Ch D 659, 665. However the subsequent decisions have gradually retreated from this stance: see *Doodeward v Spence* (1908) 6 CLR 406; *R v Kelly* [1999] QB 621; *AB v Leeds Teaching Hospital NHS Trust* [2004] EWHC 644 (QB); *Dobson v North Tyneside Health Authority* [1996] 4 All ER 474. See also Simon Douglas and Imogen Goold, 'Property in Human Biomaterials: A New Methodology' (2016) 75 CLJ 478, 479-480; Imogen Goold, 'Why Does It Matter How We Regulate the Use of Human Body Parts?' (2014) 40 J Med Ethics 3.

<sup>244</sup> See e.g. *Yearworth* (n 50 above), [31] (public health, and sacrilege); *Doodeward* (n 243 above) per Higgins J dissenting ("imperious necessity for speedy burial (or other disposition) of the dead"). There was also a logical justification for this position, specifically that if one cannot own a human body when alive, then death should not make a difference (see *Yearworth* (n 50 above) at [31]).

It is suggested that there are indeed convincing normative reasons to confer property rights in respect of digital assets, and the key argument in favour of recognising such rights is a simple one.

In essence, people who use digital assets have expectations that they can exercise the relevant transactional powers associated with the digital asset (and often pay enormous sums<sup>245</sup> to obtain digital assets under these expectations). For example, a person (X) who purchases Bitcoin expects to be able to exercise the transactional power to transfer the Bitcoin to another public address (e.g. if he wants to sell it to someone else, or transfer it to another address owned by himself).

If X is prevented from being able to exercise his transactional power (e.g. because a hacker has misappropriated his Bitcoin by transferring it to an address over which X does not have any control, or because there has been a DDoS attack that prevents X from being able to access the web interface required to exercise his transactional power), X's expectations would be defeated.

If there are no rights to sue the hacker or attacker in respect of these impairments of use of the transactional power this would result in inadequate protection for X (and anyone in X's position).

In the digital asset context, people's expectations that they should be able to exercise the relevant transactional powers<sup>246</sup> are worth protecting because the primary way in which a

---

<sup>245</sup> E.g. NFTs have been bought for millions of dollars (see e.g. 'The 29 Most Expensive Sold NFTs in the World | POWER.xyz', *POWER.xyz* at <https://power.xyz/engage/story/most-expensive-nfts/> (accessed 3<sup>rd</sup> January 2025), and many institutional players have recently bought many (i.e. hundreds or thousands of) Bitcoins for over \$100,000 each (see 'Semler Scientific Expands Bitcoin Holdings to 2,084 BTC, Boosts ATM Offering to \$150M | SMLR Stock News', *Stocktitan* at <https://www.stocktitan.net/news/SMLR/semler-scientific-announces-updated-btc-and-atm-activity-purchased-rpsv1ug6g6uj.html> (accessed 1<sup>st</sup> January 2025); Alex O'Donnell, 'Riot Platforms Buys More Than \$500 Million in Bitcoin', *Cointelegraph* at <https://cointelegraph.com/news/riot-platforms-buys-more-than-500-million-bitcoin> (accessed 1<sup>st</sup> January 2025); Investing.com, 'MicroStrategy Buys 5,262 More Bitcoins with Share Sale Proceeds', *Yahoo Finance* at <https://finance.yahoo.com/news/microstrategy-buys-5-262-more-142559226.html> (accessed 1<sup>st</sup> January 2025).

<sup>246</sup> I.e. their ability to use the digital asset.

digital asset is worthwhile to its holder lies in the ability to exercise the transactional powers. This is coupled with the fact that people often pay vast sums of money for the ability to exercise such transactional powers. Thus, the ability to exercise them is what needs to be protected.

Indeed, Bentham's justification of property rights is based on the importance of protecting and giving effect to people's expectations in respect of a thing.<sup>247</sup> Specifically, it is based on the protection of expectations that one can derive "certain advantages from a thing".<sup>248</sup> It is suggested that this applies in the digital asset context as well – people expect to be able to derive the 'advantage' of being able to exercise the transactional power, and this expectation is therefore worth protecting.

Indeed, people would be extremely disappointed and frustrated if there were no remedy in situations where their ability to exercise the relevant transactional power(s) has been interfered with or prevented.<sup>249</sup>

Thus, it is suggested that there must be a minimum level of protection for people who hold a property right to a digital asset. This would consist of a right that others do not impair his use of a digital asset in certain circumstances, and the ability to recover control of a digital asset from a person who has control of a digital asset but does not have a property right, or has an inferior property right.<sup>250</sup>

A clear case where there should be liability for impairment would be where D intentionally burns C's digital asset, knowing that he does not have title to the digital asset and

---

<sup>247</sup> Jeremy Bentham, *The Theory of Legislation* (London, 1802), 145-147.

<sup>248</sup> *ibid*, 145.

<sup>249</sup> A series of downstream consequences would foreseeably follow: people would be more likely to lose faith in crypto holdings, and less likely to hold crypto, and this may stifle future innovations in the DLT space. See also Liu, 'Crypto as property' (n 36 above) (discussion applying to the powers to alienate, create a trust and create a charge, but they also apply to non-interference rights).

<sup>250</sup> But there would be a defence if the person in control has control with the consent of a person with a property right superior to that of the claimant: see Chapter 4, Section 4.3.1 (at n 275).

knowing that C has the best title to it, and is under no mistaken belief that C has consented to the burning.<sup>251</sup>

In relation to the right to recover control, this would encompass situations where (for example) a smart contract bug accidentally transfers C's asset from C's address to D's address. In this situation, C should be able to recover control of the asset from D. There should be a duty on D to return the asset to C when asked, because it would be unfair for C to be deprived of his ability to exercise the transactional powers, given that he expects to be able to exercise such powers, and the most direct way to recover such an ability is for D to return the asset to C.

Seen in this way, the main purpose of conferring non-interference rights is to protect the right-holder's ability to exercise the transactional power(s) in respect of the digital asset (i.e. their ability to use the digital asset), as that would give effect to people's basic expectation that they are able to exercise the transactional power(s) associated with a digital asset. As mentioned, this expectation is worth protecting because the ability to exercise such powers is the primary way in which a digital asset is valuable to its holder, and people pay vast sums of money to obtain such an ability.<sup>252</sup>

### ***6.3.2 Higher risk of a free-for-all***

There is another argument in favour of recognising non-interference rights enforceable against the world in respect of a digital asset., Specifically, if there were no such rights, there would be a substantially higher risk of a free for all in relation to digital assets, as there would be

---

<sup>251</sup> Here, D's mental state is egregious, and there is a total (and permanent) impairment of C's ability to use his digital asset (given that his ability to exercise any transactional powers in relation to the digital asset have been destroyed). See also Chapter 4, Section 2.2.

<sup>252</sup> Yet this is not a general right to information (see Section 6.2.1 above), and the extent of protection can be calibrated to an appropriate level (see e.g. proposed regime under Chapter 4, Section 4 below).

fewer disincentives against perpetrating hacks and exercising violence.<sup>253</sup> The non-interference rights are necessary in order to protect people's peaceful enjoyment of digital assets.

Let us examine the alternative situation of having no property regime such that there are no rights to sue for interference in respect of a digital asset over and above what the general law affords,<sup>254</sup> and 'loss would lie where it falls'.

In the absence of a property regime, there would be a substantially higher risk of a 'free-for-all' in respect of digital assets. This occurs in two ways – one purely digitally, and one via the physical world.

First, if there are no property rights in digital assets, there would be far fewer disincentives against perpetrating blockchain and smart contract hacks, because there would be far fewer penalties under both criminal and civil law.

In terms of criminal law, there would be no liability under the *property* offences (such as theft and criminal damage) if digital assets are not *property*.<sup>255</sup> There would also be no liability under the Computer Misuse Act 1990 for most smart contract hacks because executing a smart contract function (where the code is publicly accessible) does not require unauthorised acts in relation to a computer, unauthorised access to any data or program, unauthorised execution of any program, or impairment of the operation of any computer or program.<sup>256</sup>

In terms of civil law, there would be no liability under conversion or trespass, since the chattel torts do not apply to digital assets.<sup>257</sup> There would also be no liability under trust-related

---

<sup>253</sup> Simon Douglas has made a similar argument in relation to human body parts: see Simon Douglas, 'The argument for property rights in human body parts: scarcity of resources' (2014) 40 J Med Ethics 23.

<sup>254</sup> And, by extension, no proprietary or trust-based claims (including knowing receipt and dishonest assistance).

<sup>255</sup> E.g. Theft Act 1968, s.1(1); Criminal Damage Act 1971, s.1 (cannot constitute these offences if no "property" has been dishonestly appropriated, or damaged etc).

<sup>256</sup> There would therefore be no liability under s.1 or s.3. There would also be no liability under breach of confidence or misuse of private information as there is no private or confidential information that is being disclosed or used (given that smart contract hacks generally do not involve knowledge of anyone's private key).

<sup>257</sup> The chattel torts do not apply to digital assets, and the economic torts, unjust enrichment, and the information and intellectual property torts do not provide adequate protection in the case that a digital asset is burnt or frozen: see Chapter 4, Section 2.3.

claims, e.g. constructive trusts<sup>258</sup> in respect of the asset or its substitutes (whether against the initial hacker or subsequent recipients), or knowing receipt – because there is no *property* and thus no possible trust.

The incentive to hack is high because digital assets have high market value, and if hackers can misappropriate these assets with legal impunity (or face fewer consequences when doing so), they would be more incentivised to do so. In particular, hackers (whether acting independently or in concert with others) may be assessing the likelihood of (1) being liable and/or convicted<sup>259</sup> under the criminal law, and (2) being liable and/or being ordered to pay damages (or hand over the property, proceeds, or subsequent gains)<sup>260</sup> under the civil law. They may also be assessing the expected penalty<sup>261</sup> under (1) and (2). If the likelihood of (and expected penalty under) (1) and/or (2) become substantially lower, this increases the risk that a hacker would misappropriate digital assets.<sup>262</sup> This would, in turn, be more likely to disturb the peaceful enjoyment of digital assets.<sup>263</sup>

Second, the absence of a property regime in relation to digital assets would also mean that there is a higher risk of people exercising violence in the physical world (such as via

---

<sup>258</sup> The primary remedy in the case that a digital asset is misappropriated is a constructive trust (see e.g. *Ho* (n 149 above), at [41]-[44]), which simply cannot arise if there is no (property) right over which the trust exists. If trusts and proprietary remedies are not available, the claimant may (although the position is uncertain) have a claim for breach of confidence (where the defendant has used the claimant's private key (as confidential information) to misappropriate the digital asset), but it offers a much weaker range of remedies (e.g. no tracing into substitutes, no claims against subsequent recipients, no default proprietary remedies). See also discussion in John McGhee and Steven Elliott (eds), *Snell's Equity* (35<sup>th</sup> ed, Sweet & Maxwell 2024), 9-024 (“there is little inclination for the extension of [constructive trusts] to cases where the asset acquired or created with confidential information was neither a trust asset nor a traceable product of such an asset”).

<sup>259</sup> Including the ‘practical’ aspects of whether one is likely to evade detection or escape prosecution, and thus not be convicted.

<sup>260</sup> Including the ‘practical’ aspect of whether one is likely to evade detection or the valid service of a claim form.

<sup>261</sup> Some sophisticated hackers may also be assessing the probability distribution over all possible outcomes in relation to (1) and (2).

<sup>262</sup> It lowers the threshold required for a hacker to be willing to perpetrate a hack (i.e. lowers the ‘breakeven point’ from an expected value (EV) perspective).

<sup>263</sup> See also Liu, ‘Title, control and possession’ (n 6 above), 604-605.

wrench attacks)<sup>264</sup> to try and obtain control of digital assets.<sup>265</sup> This would give people with substantial amounts of digital assets more reason to fear for their physical safety. Indeed, there have been various wrench attacks and kidnappings based on digital assets,<sup>266</sup> and if digital assets are not recognised as property, physical attacks and kidnappings would be more likely to occur.<sup>267</sup>

Nonetheless, in relation to the second point, one may argue that existing criminal law and tort law already provide protection in respect of violence (namely via the offences against the person<sup>268</sup> and the tort of trespass to the person), and so there are already disincentives against exercising violence to obtain control of a digital asset. However, it is suggested that these forms of protection do not sufficiently address the increased risk of a free-for-all in the absence of a private law property regime.

Apart from the fact that the lower penalties in civil and criminal law still provide an increased incentive for such violence to occur,<sup>269</sup> there is an additional reason, analogous to that given by Rostill In the physical asset context.

In the physical asset context, a property right (in the sense of private law non-interference rights) confers more stability and security on possessors, and reduces the situations that are “conducive to the risk of violence”,<sup>270</sup> relative to where there are only criminal and tort

---

<sup>264</sup> A wrench attack is where someone with large cryptocurrency holdings (X) is physically threatened or attacked by another person (Y) in order for his private key(s) to be disclosed to Y.

<sup>265</sup> Liu, ‘Title, control and possession’ (n 6 above), 604-5. In addition, there would also be a higher risk that people would look for seed phrases or private keys that are ‘lying around’ (e.g. left on a Post-it note or other piece of paper) and misappropriate the relevant cryptoasset(s) without violence.

<sup>266</sup> See e.g. Liam ‘Akiba’ Wright, “Kidnappings and home invasions highlight need for enhanced physical security in crypto”, *CryptoSlate* available at <https://cryptoslate.com/kidnappings-and-home-invasions-highlight-need-for-enhanced-physical-security-in-crypto/> (accessed 30<sup>th</sup> August 2024); Zhiyuan Sun, “\$5 wrench attacks appear to be on the rise in the crypto community”, *Cointelegraph* available at [cointelegraph.com/news/5-wrench-attacks-appear-to-be-on-the-rise-in-the-crypto-community](https://cointelegraph.com/news/5-wrench-attacks-appear-to-be-on-the-rise-in-the-crypto-community) (accessed 30<sup>th</sup> August 2024).

<sup>267</sup> The reduced penalties under civil and criminal law mentioned immediately above (see nn 255-258 above and text thereto), provide increased incentives for such violence, since (e.g.) the defendant(s) are less likely to have to hand over their gains, especially if there are subsequent recipient(s). The points in the previous paragraph also apply here.

<sup>268</sup> Assault and battery.

<sup>269</sup> See n 267 above.

<sup>270</sup> Rostill (n 47 above), 29.

law prohibitions on violence. If there were no such rights (such that non-violent takings would be lawful), this would still substantially increase the risk of violence. For example, a person (D) may not initially intend to use violence to take a physical asset, but the attempt to take the asset (and the subsequent resistance from the person in possession) may end up escalating into a violent struggle.<sup>271</sup> During the period of escalation, D is not likely to be thinking rationally about the criminal and tort law penalties that would ensue from exercising violence, and is instead likely to be motivated by the pure emotional desire of obtaining possession of the asset – hence the increased risk of violence relative to if there were property rights to physical assets.

Similarly, in the digital asset context, if there were no property rights to digital assets, a person (D) may wish to (lawfully) take C’s digital assets, and attempt to persuade C to (e.g.) type his private key or seed phrase into the wallet<sup>272</sup> application on D’s computer,<sup>273</sup> without using violent means. If C resists and/or acts defensively, the situation may escalate in a way where D may resort to violent means to obtain C’s private key (such as via a wrench attack). He may also threaten to use violence, which may escalate into actual violence.<sup>274</sup>

At this point, one may argue that classifying digital assets as property under the criminal law would be sufficient to solve the ‘free-for-all’ problem, on the basis that there would be criminal penalties for acts such as intentional destruction of a digital asset.

However, this would be insufficient because the criminal law does not provide a ready mechanism for remedies to be granted to the *claimant* in an adequate range of situations.<sup>275</sup>

---

<sup>271</sup> *ibid.*, 29; see also Amy Goymour, “Bruton v London & Quadrant Housing Trust [2000]: Relativity of Title, and the Regulation of the ‘Proprietary Underworld’”, in Douglas, Hickey and Waring (eds), *Landmark Cases in Property Law* (Hart Publishing, 2015), 151, 172. Goymour argues that there would be a “free-for-all in the proprietary underworld” if there is no relative title doctrine. By extension therefore, there would be a free-for-all if there are no non-interference rights.

<sup>272</sup> E.g. MetaMask, which is a software wallet for digital assets on the Ethereum blockchain.

<sup>273</sup> Such that D would have access to C’s digital assets and be able to transfer them to his own address.

<sup>274</sup> The same point about D not being likely to be thinking rationally (about potential penalties resulting from his violent conduct) during the period of escalation also applies here.

<sup>275</sup> For the importance of the claimant having the right to sue to redress wrongs, see John CP Goldberg and Benjamin C. Zipursky, *Recognizing Wrongs* (Harvard University Press, 2020); Andrew S Gold, *The Right of Redress* (OUP, 2020).

Issues such as prosecutorial discretion and limited public resources pose obstacles for a claimant who is trying to recover (e.g.) the digital asset that has been misappropriated via a smart contract hack (or its value), in circumstances where there has been no violence.<sup>276</sup> This means that protection under the civil law is required for the claimant to be able to recover the asset (or its value) under a reliable legal mechanism that is specifically directed towards providing remedies to the claimant.

As such, in order to prevent (or substantially reduce the risk of) potential free-for-alls in respect of digital assets, having a property regime that imposes (at least) duties of non-interference that are directed towards the digital asset would be infinitely preferable to not having one.

The level of legal protection in respect of a digital asset thus cannot just be the same as a ‘valuable piece of information’, contrary to Stevens.<sup>277</sup> Fundamentally, the ‘pure information’ level of protection does not address the risk of a free-for-all, because it does not provide adequate protection where there is misappropriation<sup>278</sup> of a digital asset by changing control of it. Many misappropriations happen without use or disclosure of the private key,<sup>279</sup> and in such cases there is no possible recourse via any of the ‘information torts’ such as misuse of private information.<sup>280</sup>

This may be in part because from a conceptual perspective, pure information simply *cannot* be misappropriated, given that it is not rivalrous. It is therefore no surprise that the remedies addressing the protection of information do not adequately cover misappropriation of

---

<sup>276</sup> For example, he cannot successfully sue for trespass to the person because there is no violence. There are also no default remedies under the economic torts, chattel torts, unjust enrichment, or the information torts. Also, the absence of a property right means that in the event of a misappropriation, the claimant cannot trace into substitute assets or recover the property under a constructive trust (against the initial wrongdoer or subsequent recipients), or sue for knowing receipt.

<sup>277</sup> Stevens (n 34 above), 621.

<sup>278</sup> This is the case not only for misappropriation. There is also a lack of protection when a digital asset is burnt or frozen: see e.g. Liu, ‘Interference torts’ (n 36 above), section 2.

<sup>279</sup> E.g. smart contract hacks.

<sup>280</sup> Liu, ‘Interference torts’ (n 36 above), section 2.

a digital asset – unlike pure information, a digital asset is a rivalrous asset that is capable of involuntary alienation and destruction.

At the same time, as mentioned earlier,<sup>281</sup> imposing non-interference rights that are directed at the digital asset would not be overly harsh on defendants, since (1) such rights do not amount to a general exclusive information right but are rather rights to sue for interference with a particular rivalrous object (and/or its use), and (2) the conditions of liability can be calibrated in a way that are defendant-friendly enough (such as by imposing defendant-friendly mental requirements). The effects of such non-interference rights on the liberty of third parties can thus be carefully controlled, and there would not be liability on the mere basis that (e.g.) someone discovers a private key, just as there would be no liability where someone discovers where a pot of gold is buried.

## **7. Conclusion**

This chapter has established the following main points. First, that the ‘digital assets’ that will be explored in this thesis involve factual power(s) to make transactions on a permissionless blockchain ledger, including the ability to transfer. Second, that ‘property’ for the purpose of this thesis will denote non-interference rights effective against the world, because they are fundamental to protecting a person’s ability to use their digital asset(s). Third, that there exists a significant gap in the case law where none of the four research questions have been explored in detail, and the courts have not been asking the correct questions. Fourth, that it is conceptually possible to have property rights in respect of digital assets. Fifth, that it is normatively desirable to have such rights.

---

<sup>281</sup> See Section 4.1 above.

The next chapter will explore the appropriate threshold for when a person should acquire such rights for the first time, and how best to describe this threshold from a doctrinal perspective.

## **Chapter 2: Acquisition of a property right**

### **1. Introduction**

Chapter 1 has established that digital assets are conceptually capable of being the subject-matter of a property right, and that it is normatively desirable to for a legal system to offer the possibility of a party having a property right<sup>1</sup> in respect of a digital asset.

This chapter will explore the question of what the threshold for acquiring an original property right to a digital asset should be, and how this threshold should be described (possession or control). An ‘original’ property right refers to a property right that one independently acquires, as opposed to one that is acquired from someone else.<sup>2</sup>

It will be argued that one should acquire an original property right in respect of a digital asset when one has positive and negative control of a digital asset, coupled with an intention to exercise control over the digital asset.

This is because (1) this threshold is analogous to the threshold for acquisition of original title to a physical asset, and (2) the justifications for the threshold for acquiring an original title to physical assets apply equally to digital assets, so that it would be arbitrary to not confer an original title (and thus *a fortiori* an original property right) in relation to the latter.

It will also be argued that the concept should be used to describe this threshold is ‘control’, instead of ‘possession’.

---

<sup>1</sup> I.e. non-interference rights exigible against the world (meaning 2): see Chapter 1, Section 3.2.

<sup>2</sup> Acquiring a new and original right is also ‘independent’ acquisition, as opposed to ‘dependent’ acquisition (acquiring a pre-existing right from another person): see Simon Douglas, *Liability for Wrongful Interferences with Chattels* (Hart Publishing, 2011), 29.

Section 2 will explore the normative question (the appropriate threshold for acquiring an original property right to a digital asset), and Section 3 will explore the doctrinal question (the legal test that should be used to describe such a threshold).

## **2. The normative question**

This section will argue that an analogy can be drawn between possession of a chattel and (positive and negative) control of a digital asset, such that they should generally be seen in the same light for the purpose of the acquisition of title rules.<sup>3</sup> It will also argue that the similarities between physical and digital assets are such that the justifications for conferring a title on a person who acquires possession of a chattel extend to conferring title (and thus a property right)<sup>4</sup> on a person who has control over a digital asset.

In reaching this conclusion, I will first explore the ‘factual element’ (positive and negative control) and then the ‘intention element’ (intention to exercise control over a digital asset) that needs to be satisfied for title to arise. After this, I will explore the justifications for the possession rule in respect of physical assets and explain why the justifications apply across to digital assets.

### **2.1 Property rights to digital and physical assets**

This section uses physical assets as a reference point for the analysis as to when an original property right ought to arise in respect of a digital asset, and this is because there are various similarities between a property right in a digital asset and a property right in a physical asset.

---

<sup>3</sup> Original acquisition.

<sup>4</sup> As a property right is a subset of title (see Chapter 1, Section 4.3.1).

Crucially, the content of the non-interference right is shaped by the ‘thing’ or ‘asset’ (whether physical or digital), and such an asset is rivalrous, and independent of the legal system and other persons. This contrasts with rights/duties that are defined by prohibited actions (such as copyright infringement, or the economic torts) without reference to a distinct rivalrous ‘thing’ that is independent of the legal system and persons. Thus, using physical assets (and property rights thereto) as a point of reference is an appropriate starting point.

It is suggested that one should acquire an original property right to a digital asset when he has positive and negative control over the digital asset, plus an intention to exercise control over the digital asset.

Linking this back with the Chapter 1 discussion of ‘aim, substance and technique’,<sup>5</sup> this argument involves an analogy with physical assets at the ‘substance’ level instead of the ‘technique’ level, since the analogy is drawn with the threshold required to obtain title. The later discussion (in Section 3) will in fact involve a distinction at the ‘technique’ level because despite the proposed acquisition of title threshold being the equivalent of that in the physical asset context, the doctrinal term or technique that should be used (‘control’) diverges from the term used in the physical asset context (‘possession’). Nonetheless, the ‘aim’ of ascertaining the appropriate threshold for the acquisition of original property rights remains the same across physical and digital assets – namely to confer such rights in appropriate circumstances without unduly stifling the liberty of third parties.

### ***2.1.1 The ‘core’ case, and positive and negative control***

It is suggested that the ‘core’ case in which a person should acquire a property right to a digital asset is when it is ‘minted’ into a public address over which that person has positive and

---

<sup>5</sup> Introduction, Section 2.1 above.

negative control. This is provided that there is an intention to exercise control over the digital asset (which will be discussed in more detail in Sections 2.1.2 and 2.2.5); this section will focus on the factual requirement of positive and negative control).

This ‘core’ case typically occurs where a digital asset is ‘mined’ in a proof-of-work cryptocurrency or deposited into one’s wallet address under a proof of stake<sup>6</sup> consensus protocol. An example would be where a miner mines Bitcoin, and the coin is deposited in such an address. Indeed, the Law Commission note that “mining a crypto-token (either in a proof of work or a proof of stake system) would<sup>7</sup> result in a new, independent acquisition of [title to] the crypto-token that the miner or staker receives”.<sup>8</sup>

This is the general expectation amongst people in the crypto-community,<sup>9</sup> as people expect to obtain title to a digital asset for the first time where it is deposited in his or her address.<sup>10</sup> As mentioned, this ‘title’ encompasses a property right as well as various powers in respect of it (e.g. the power to alienate, and create a trust or charge over it).<sup>11</sup>

In this scenario, one should acquire a property right<sup>12</sup> to the relevant digital asset because (1) it is analogous to how someone acquires an original title to a physical asset (which includes a property right to it, and (2) the justifications for conferring an original title in respect of a physical asset apply equally to digital assets such that it is arbitrary to confer an original title in respect of one type of asset but not the other (explored in Section 2.2 below).

---

<sup>6</sup> There are many other consensus algorithms, such as Delegated Proof of Stake, Proof of Authority, and Proof of Elapsed Time.

<sup>7</sup> The Law Commission say ‘would’, but the point has not been tested so it is more accurate to say ‘should’.

<sup>8</sup> Law Commission of England and Wales, *Digital Assets: Consultation paper* (Law Com No 256, 2022), 13.16. The important fact here is not the mining or staking *per se*, but that the miner or staker obtains positive and negative control of the token they receive. Positive and negative control are discussed below: see Section 2.1.1, paras 6-10 below.

<sup>9</sup> This observation is based on the author’s interactions with industry participants for the last four years.

<sup>10</sup> At least when they have an intention to exercise control over the asset on their own behalf. Some people may expect to obtain title to a digital asset when it arrives into the address *per se*, but it is suggested that they should not do so until they have an intention to exercise control over it on their own behalf (see sections 2.2.5 and 2.1.2 below).

<sup>11</sup> As they expect to obtain title, they expect (*a fortiori*) to obtain a property right.

<sup>12</sup> Provided that the necessary intention exists (discussed at Sections 2.1.2 and 2.2.5 below).

The rule for physical assets is that one acquires an original title in respect of it if one is in physical possession of it with an intention to possess it in one's name and on one's own behalf.<sup>13</sup> As mentioned earlier, title to a physical asset encompasses a property right in respect of it, plus various powers in relation to the right.<sup>14</sup> This title is exigible against the world except those with a better title.<sup>15</sup> Thus, if one acquires an original title in a physical asset, he would *a fortiori* acquire a property right in it, and this title would be exigible against the world except those with a better property right.

Physical possession denotes exclusive physical control,<sup>16</sup> which requires negative control (the ability to exclude others from the asset) and positive control (the ability to exercise the uses associated with the asset).<sup>17</sup> Of course, the extent of positive and negative control required varies according to the physical asset in question: for chattels, the level of control required is generally higher than that for land. It is not possible, for example, to have the same degree of control over a house as compared to a phone.<sup>18</sup>

Similarly, in the digital asset world, having a token deposited in one's address means that one has positive and negative control. In relation to positive control, the tokenholder has the ability to execute an on-chain transfer of the asset to another address (which divests him of his coin and allows another person to have the same positive control), and (if the program allows) also has the ability to obtain any benefits associated with holding the coin (e.g. the

---

<sup>13</sup> See Luke Rostill, *Possession, Relative Title, and Ownership in English Law* (OUP, 2021), 15 (and in particular fn51), and Chapter 2 generally.

<sup>14</sup> Chapter 1, Section 4.3.1 above; Rostill (n 13 above), 112-113 and chapter 5 generally.

<sup>15</sup> The strength of the title can vary (as there can be ownership (or the 'best' title) as well as inferior titles). Title to a chattel is also referred to as a 'general property interest': see generally Rostill (n 13 above), 112-113 and Luke Rostill, 'Terminology and Title to Chattels: A Case against 'Possessory Title'' (2018) 134 LQR 407.

<sup>16</sup> In a factual sense (factual control) as opposed to a legal sense (legal control). Factual control refers to the position where we ignore the legal relationship between the parties, whereas legal control refers to whether as a matter of law, one has the right to obtain control of the asset from another person, or prevent another person from exercising control over the asset.

<sup>17</sup> See e.g. *Powell v McFarlane* (1977) 38 P&CR 452 (Ch) 471; Rostill (n 13 above) 15-19.

<sup>18</sup> Indeed, "not all objects are amenable to the same types of control": see William Vaudry and Sarah Green, 'Electronic trade documents: the Law Commission's provisional proposals, the MLETR, and the concept of possession' (2021) 8 JBL 625, 631-632. Also see Michael Crawford, *An Expressive Theory of Possession* (Hart Publishing, 2020), 62-63; Rostill (n 13 above), 16-19; Law Commission of England and Wales, *Electronic trade documents: Report and Bill* (HC 1188, Law Com No 405, 16 March 2022), 5.28-5.45.

power to vote, bid, receive an airdrop, execute in-game actions, or mint a token, via a blockchain transaction).<sup>19</sup>

The ‘positive uses’ that can be made of a blockchain token are generally much more limited than the uses that can be made of most physical objects. For example, a football can be used in many ways: one can (e.g.) hold or touch a football using various body parts, move it around with one’s feet, or draw all kinds of objects on it. In contrast, a blockchain token can only be ‘used’ by accessing it with one’s private key, and signing blockchain transactions using it, including transferring it to various designated locations (public addresses).

In relation to negative control, the wallet holder has the ability to exclude people from accessing and transferring the asset because he has a private key. This is the maximum degree of control allowed by the asset, and would amount to the digital equivalent of ‘possession’. As such, the analogy between physical and digital assets can be established insofar as there can be positive and negative control over a digital asset.

Therefore, if one can use the private key to exercise the relevant functionalities associated with the digital asset (positive control), and prevent others from exercising such functionalities (negative control), then this would satisfy the equivalent of the factual threshold of control required to obtain title to a physical asset.

#### 2.1.1.1 Multi-signature addresses

Thus far, the assumption has been that the relevant digital asset is deposited or minted into a single-signature address, i.e. an address that only has one private key. The other type of address is the multi-signature address.

---

<sup>19</sup> However, extra actions such as voting and redemption are not *necessary* for positive control to exist.

A multi-signature address is an address where there are N private keys in total (e.g. 3), and the execution of a blockchain transaction requires signatures from M private keys (e.g. 2). These addresses are typically used as part of shared control arrangements that place restrictions on an individual's ability to exercise positive or negative control. Of course, a multi-signature address can also be used by one person (e.g. if someone wants to set up a 2 of 3 multisig for himself, so that he is not prevented from executing a blockchain transaction even if he loses one of the keys). However, the majority of multi-signature addresses involve shared control scenarios.

In shared control scenarios, a multisig address places restrictions on at least one person's ability to exercise positive or negative control. For example, in a 3 of 3 multisig arrangement where A, B and C each have one key, signatures from all three people would be required in order for a digital asset to be transferred out of the address. In this case, each person can exercise negative control (as each person can prevent a transfer by refusing to sign), but not positive control (as each person does not have the unilateral ability to execute a transfer). Another example would be a 1 of 2 multisig arrangement, where A and B each have one key but a digital signature from one would suffice to transfer the digital asset. In this case, both A and B can exercise positive control (the unilateral ability to execute a transfer), but neither of them has negative control (the ability to prevent a transfer). Nonetheless, in both cases, the parties (A, B and C in the first example, and A and B in the second example) jointly have positive and negative control.

Where a digital asset is deposited into a multi-signature address, it is suggested that the appropriate threshold to obtain an original property right is to have enough keys to be able to exercise negative control, and enough keys to be able to exercise positive control. This threshold should apply irrespective of whether the address is a single-signature or multi-signature address.

Specifically, in a M of N multisig arrangement (i.e. where there are N keys, and M keys are required to execute a blockchain transaction), one needs the higher of: (1) M keys (the threshold for positive control), and (2) one more than N-M keys (the threshold for negative control).

For example, in a 1 of 3 multisig address, the threshold for positive control is 1 key (M), and the threshold for negative control is 3 keys ( $N-M = 3-1 = 2$ , and one more than that is 3). This means a person needs all three keys to obtain a property right to the relevant digital asset. If a person (A) only has 2 keys, the person with the other key (B) can unilaterally execute a transaction on the blockchain (exercise positive control), with the result that A has no negative control because he cannot prevent B from executing transactions on the blockchain.

In a 2 of 3 multisig address, the threshold for positive control is 2 keys (M), and the threshold for negative control is 2 keys as well ( $N-M+1 = 3-2+1 = 2$ ). He needs two keys to obtain a property right to the relevant digital asset.

If a person has enough keys for positive control (i.e. M keys) but not negative control (i.e.  $N-M+1$  keys), it is suggested that the law should not confer a property right to the digital assets. This is consistent with the threshold in relation to physical assets, where if someone does not have negative control of a physical asset then he does not acquire an original title to it.<sup>20</sup>

Nonetheless, it is not necessary for any one person to have the required number of signatures to obtain a property right, if control is exercised jointly. For example, in the context of a 2 of 2 multisig address, the threshold for obtaining a property right to a digital asset in such an address is 2 keys,<sup>21</sup> but if A and B each hold one key and exercise joint control, then A and B obtain a joint property right to the digital asset.<sup>22</sup>

---

<sup>20</sup> See text to nn 13-18 above; negative control is required.

<sup>21</sup> The threshold is 2 because  $M = 2$ , and  $M-N+1 = 1$ ; the higher (of 2 and 1) is 2.

<sup>22</sup> This is the same for single signature addresses where the key is sharded (i.e. split up into multiple fragments, and each party has one of the fragments), and the parties exercise joint control.

### 2.1.1.2 Theft

There would also be positive and negative control where a digital asset is stolen by a hacker and transferred into his own public address<sup>23</sup> because the result would be that he has negative control (because he can exclude others from access by way of private key(s)) as well as positive control (because he can execute an on-chain transfer of the asset and obtain other possible benefits programmed into the asset). This raises the question of whether the hacker or thief should obtain a ‘relative’ title, which will be explored later.<sup>24</sup>

### 2.1.1.3 Boundary issues

Of course, there are ‘boundary’ issues as to (for example) how many block confirmations<sup>25</sup> are required before one obtains positive and negative control of a digital asset, as the risk of (for example) a block being subsequently orphaned needs to be taken into account.<sup>26</sup> These issues are, of course, not unique to digital assets, as there are also uncertainties as to when one obtains possession of a physical asset too.<sup>27</sup>

It could be argued that there is also a boundary issue relating to ‘burn permissions’ where a third party has the power under a smart contract to burn someone’s digital asset. If someone can have the unilateral power to burn such an asset, this raises the question of how

---

<sup>23</sup> Where he would have the required number of keys for positive and negative control (one if it is a single-signature address, and ‘the higher of ‘M’ and ‘M-N+1’ if it is a multi-signature address).

<sup>24</sup> See Section 2.2 para 1 below, and Sections 2.2.3 and 2.1.2 below.

<sup>25</sup> When a block is confirmed as valid, every subsequent block that is mined on top of such a block counts as an extra ‘confirmation’.

<sup>26</sup> An orphaned block is a block that is confirmed as valid but is not accepted on the main chain, and thus cannot be used on the main chain or network.

<sup>27</sup> Possession demands a fact-specific inquiry, and the degree of control required to constitute possession varies from object to object: see n 18 above. It is difficult to pinpoint (in respect of each chattel) the exact threshold at which one obtains possession.

much control over a digital asset can in effect be exercised by a tokenholder, since it can be destroyed by a third party. In this regard, it is suggested that this is a non-issue as far as factual negative and positive control are concerned. Even in the physical asset context, I may have title to a fragile object that can be destroyed easily by a third party. I can move it around and exclude others from using it, for example by locking it in a safe. Similarly, in the digital asset context, burn permissions are still consistent with the tokenholder having factual positive and negative control since the tokenholder can still (1) execute an on-chain transaction and (2) use his private key to exclude hackers from accessing or transferring the asset.

How about situations where a smart contract limits the amount of control that a person can exercise in respect of a digital asset at a given time? For example, there could be an asset that is deposited or minted into a smart contract address where there are restrictions on one's ability to execute an on-chain transfer of the asset, based on (for example) a time-based restriction (e.g. no transfers allowed until 1<sup>st</sup> June 2025), or an act-based restriction (e.g. presentation of conforming documents). It is suggested that the same threshold applies – i.e. if the person has enough signatures to have negative control as well as the required number of signatures to execute a transaction<sup>28</sup> on the blockchain, he should obtain title to the digital asset.<sup>29</sup> This is because there are valuable uses that need to be protected in respect of the digital asset. First, there is the need to protect C's ability to execute an on-chain transfer of the asset in the future when the restriction on such transfer is lifted. Second, even in the period before the restriction on transfer is lifted, there may be functionalities such as voting, bidding, redemption entitlements, and the ability to mint. This remains the case irrespective of whether there are restrictions on one's ability to execute an on-chain transfer of the asset.<sup>30</sup>

---

<sup>28</sup> Which encompasses transactions that he can only enter into in the future.

<sup>29</sup> Provided there is an intention to exercise such control on one's own behalf.

<sup>30</sup> The Law Commission (in its Final Report) recommended the creation of a technical expert group to advise on issues related to control: see Law Commission of England and Wales, *Digital Assets: Final report* (HC 1486, Law Com No 412, 2023), 5.23-5.37. This would help to shed light on the factual context behind various types of digital asset arrangements, and whether there is positive and/or negative control under such arrangements.

Under Article 11 of the DAL,<sup>31</sup> one does acquire an original title in ‘smart contract limited control’ situations where he has the number of private keys that allow him to have positive and negative control.

### ***2.1.2 The intention requirement***

Apart from having the threshold of factual control described above, it is suggested that one must also intend to exercise control of the digital asset on his own behalf to obtain an original property right to it.

Where a person has positive and negative control of a digital asset, there is typically also an intention to exercise exclusive control<sup>32</sup> over such asset on one’s own behalf.<sup>33</sup> Where a digital asset is mined under a proof-of-work system, the act of running the computer operations/calculations to solve the relevant puzzle would clearly indicate an intention to exercise control over the mined coin. Similarly, under a proof-of-stake system, opting in to the system of validating blocks would also indicate such an intention.

However, there should not be a requirement that he must intend to control the asset for his own ultimate *benefit*.<sup>34</sup>

In the case where a trustee (T) takes exclusive control of a (physical or digital) asset that is intended to be held on trust, it would be difficult to say that he takes control of it for his

---

<sup>31</sup> DIFC’s Digital Assets Law (DIFC Law No. 2 of 2024) (“DAL”), Article 11(1); see also Articles 10(1) and 10(3)(a).

<sup>32</sup> Exclusive control ie positive and negative control.

<sup>33</sup> The issue of ‘own’ behalf also depends on the capacity in which one acts (as an individual or for a company etc).

<sup>34</sup> To the extent that are suggestions that the threshold (in the physical asset context) requires an intention to control the asset for one’s own benefit (see e.g. *Mainline Private Hire Ltd v Nolan* [2011] EWCA Civ 189 (at [1])), it is suggested that this is misleading. In the ‘trustee’ case explored below, the claimant ultimately intends to control the asset for the benefit of the beneficiary (and not for his own benefit), yet the law would probably confer title on the claimant.

‘own benefit’. This is because T all along intends to take control of the asset for the benefit of the beneficiary.

Yet, although there is no case law on this point, the law is likely to provide T with the ability to sue for interference in the physical asset context, and in the digital asset context the same threshold should be adopted. T is in (factual) exclusive control of the asset, and intends to take exclusive control over it.<sup>35</sup> In relation to whether he intends to take exclusive control over it ‘in his own name and on his own behalf’, he does not take the asset as agent for (e.g.) his master/principal, or in any capacity where he is the mere instrument of another’s power, in which case there would not be the requisite intention to control.<sup>36</sup> This would be the case whether the asset is physical or digital.

Thus, there is a strong argument that the intention element is satisfied. The opposite outcome would mean that a trustee (or intended trustee) of a self-declared trust can never achieve the effect of holding an asset of which he obtains factual control on trust, because he would not obtain title to the asset so would not be able to declare anything on trust. If a person intends to possess an asset as trustee of a self-declared trust, he would have to obtain (an original) legal title to the asset *before* declaring it on trust: there will necessarily be a *scintilla temporis* between the moment he obtains legal title to the asset and the moment it is held on trust. If one does not obtain legal title to the asset where he intends to possess it as trustee of a self-declared trust, this would defeat the very purpose for which the person obtains possession, since there would simply be no legal title to hold on trust.

Requiring exclusive control to be taken for one’s *benefit*<sup>37</sup> would therefore seem to produce a narrower rule than the current law. Thus, to the extent that the case law on the

---

<sup>35</sup> The justifications mentioned in Section 2.2 do not seem to apply any less to this situation (relative to ‘core’ situations that do not involve trusts or agency).

<sup>36</sup> Acquiring as trustee is different from acquiring as agent, because in the latter case one is not acquiring the asset on behalf of (or in the capacity of) himself, but rather his principal.

<sup>37</sup> In a way that does not cover control by an (intended) trustee of an asset that he seeks to immediately hold on trust.

possession rule for chattels suggests that one needs to exercise exclusive possession (or control) for one's own benefit,<sup>38</sup> it should be read as synonymous with 'own behalf' as opposed to adding an additional requirement, in order to provide clarity of application in the digital asset context. The concept of one's own behalf (as opposed to one's benefit) concerns the issue of 'capacity' as opposed to who the ultimate beneficiary of the act would be.

In the physical asset context, the justification for an intention requirement is clear. If one does not intend to control the item in question, it is difficult to see why the law should confer on him a title to sue for interference. If one does not intend to use and control the asset, there is nothing 'unjust' in a third party (e.g.) taking the asset for its own use.<sup>39</sup> This reasoning also explains why there is a requirement to control the asset in one's name and on one's own behalf, since if I intend to control the asset on behalf of someone else, I do not intend to exercise such exclusive control for myself (and so there is no particular reason why third parties should be under a duty to *me* not to interfere with the asset). It is the other person who intends to exercise control over the asset and uses me as an instrument for his exercise of factual control (and as such, *he* obtains title).<sup>40</sup> In this sense, the rationale of the intention requirement is also to do with the need to ascertain the party to which the law should attribute possession. As a matter of logic, these reasons apply in equal measure to digital assets.

## 2.2 Justifications for conferring title

As the 'digital equivalent' of the conditions required to acquire title to a physical asset (exclusive control and the associated intention to exercise such control) can be satisfied, this raises the important question of whether one *should* obtain title<sup>41</sup> in such circumstances. 'Title'

---

<sup>38</sup> E.g. *Mainline Private Hire* (n 34 above), [1].

<sup>39</sup> See also Section 2.2.5 below (and especially the 'likelihood' argument at Section 2.2.5, para 5).

<sup>40</sup> He has factual control through using me as an agent or instrument.

<sup>41</sup> And thus, a fortiori, a property right.

includes *relative* titles i.e. original titles that are inferior to the ‘best’ title: such a title can be obtained for example by a thief who obtains possession of an asset with the requisite intention to possess.<sup>42</sup>

To this end, the underlying justifications for original title in the physical asset context need to be set out, with a view to ascertaining whether they apply to digital assets. It is argued that to the extent that the justifications for title apply to physical assets, they also apply equally to digital assets,<sup>43</sup> such that it would be arbitrary to distinguish between physical and digital assets in such way.<sup>44</sup>

### ***2.2.1 Free-for-all***

First, it has been argued that conferring title to a physical asset in circumstances constituting ‘possession’ (with an intention to possess) is necessary to prevent a free-for-all. If the law does not confer protection in the form of a general property interest that entitles the possessor to sue strangers for tortious interference, this would encourage (violent and non-violent) dispossessions by such strangers, and there would not be peaceful enjoyment of property.<sup>45</sup> Seen in this sense, granting a general property interest would be the ‘lesser of the two evils’.

The concern to prevent a free-for-all (whether violent or not) also applies in the digital asset context. If people know that (for example) a cryptocurrency has been stolen and the thief does not have title to the cryptocurrency despite him having ‘possession’ and the intention to possess, they would be encouraged to either hack the relevant blockchain, or physically try to

---

<sup>42</sup> *Costello v Chief Constable of Derbyshire Constabulary* [2001] EWCA Civ 381, [2001] 1 WLR 1437.

<sup>43</sup> I will focus on the factual element since the mental element has already been discussed in section 2.1.2 above, and will be elaborated further section 2.2.5 below.

<sup>44</sup> In other words, I am arguing that the justifications people have given for the acquisition of title threshold in the physical asset context also apply in the digital asset context, instead of arguing that these are good justifications in general.

<sup>45</sup> Amy Goymour, ‘*Bruton v London & Quadrant Housing Trust* [2000]: Relativity of Title, and the Regulation of the ‘Proprietary Underworld’ in Simon Douglas, Robin Hickey and Emma Waring (eds), *Landmark Cases in Property Law* (Hart Publishing, 2015) 151, 172; Rostill (n 13 above), 28-30.

track the person down and force him to disclose (or type in)<sup>46</sup> his private key or seed phrase.<sup>47</sup> Indeed, there have been many wrench attacks<sup>48</sup> and kidnappings of people who have large cryptocurrency holdings,<sup>49</sup> and this is in addition to the numerous blockchain hacks that do not involve any form of physical violence.

The public nature of blockchains<sup>50</sup> means that it can in fact be *easier* to identify a stolen asset, since the transactional record is public and people may more easily identify the coin that has been stolen. This can make targeted attacks easier, as people can in many cases discover the identity of the wallet holder: pseudonymity is certainly not anonymity.<sup>51</sup> Against this, it may be said that successfully wrench attacking someone is harder than taking a physical asset by force, but violence would still occur in the case of a failed wrench attack, and the thief would still need to fear for his physical safety.<sup>52</sup> Thus, the general concern to prevent a free-for-all applies to the same extent in the digital asset context.

### **2.2.2 Limitation periods**

---

<sup>46</sup> E.g. into an application such as MetaMask.

<sup>47</sup> See generally the arguments at Chapter 1, Section 6.3.2 above.

<sup>48</sup> A wrench attack is where a person with large cryptocurrency holdings is physically threatened or attacked in order for his private keys to be handed over to the attacker.

<sup>49</sup> See e.g. Zhiyuan Sun, '\$5 wrench attacks appear to be on the rise in the crypto community', *Cointelegraph* (<https://cointelegraph.com/news/5-wrench-attacks-appear-to-be-on-the-rise-in-the-crypto-community>, accessed 23rd March 2022).

<sup>50</sup> Specifically permissionless blockchains (which are the blockchains explored for the purpose of this thesis), as opposed to permissioned blockchains. Permissionless blockchains are where the majority of digital assets (and the majority of their value) is held.

<sup>51</sup> It is possible to trace the trail of transactions and eventually discover who is the owner of a particular wallet address, for example by using the technique of 'clustering': see e.g. Mengjiao Wang, Hikaru Ichijo and Bob Xiao, 'Cryptocurrency Address Clustering and Labeling' (2020) (at <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiPzt6AueD2AhU5yYsBHUqoD81QFnoECAgQAQ&url=https%3A%2F%2Farxiv.org%2Fpdf%2F2003.13399&usq=AOvVaw3-Ms06DTwyqzU27QP4wu2B>, accessed 23rd March 2022).

<sup>52</sup> And as for situations that do not involve violence (i.e. 'pure' blockchain and smart contract hacks), the fact that the blockchain and smart contract code is accessible to the public means that anyone can attempt a blockchain or smart contract hack.

The ‘free-for-all’ justification is related to limitation periods. In the chattels context (and the unregistered land context), an owner or title-holder who seeks to recover his property (or bring a claim in conversion) needs to sue within a certain period (the general rule being 6 years for chattels, and 12 years for unregistered land).<sup>53</sup> If the owner fails to bring his claim within the required period, his title is extinguished. Thus, in order to avoid the situation where no one has title to the property (meaning that the property in question would be unutilised or under-utilised), the law confers title or a ‘general property interest’ to avoid (in Battersby’s words) a “proprietary vacuum”.<sup>54</sup> Also, the extinction of title rules simply would not perform their function without a rule that confers title upon a possessor. In the adverse possession context for example, one objective is to ensure certainty as to who has good title.<sup>55</sup> Although the extinction of title rules aim to ensure certainty by limiting the time period over which one can ‘sit on his rights’, it is not enough to extinguish title after 12 years. The system also needs to ensure that the possessor has a sufficiently good title to alienate.<sup>56</sup> In the absence of such a rule, the land in question will be under-utilised because people would not be certain about whether the possessor has any rights. This would defeat the main purpose of the extinction of title rule (to provide certainty), and there would be a risk of a (violent or non-violent) free-for-all in relation to the particular asset. The same applies to chattels.<sup>57</sup> In this sense, the justification for a general property interest may ultimately relate back to general ‘efficiency’ justifications for the recognition of property rights.<sup>58</sup>

The ‘proprietary vacuum’ and ‘performance of function’ arguments would also apply equally to digital assets if there is a limitation provision in respect of the recovery of a digital

---

<sup>53</sup> Limitation Act 1980, ss. 3, 15 and 17. Nonetheless, in respect of chattels, the limitation period does not run against a thief and for theft-related conversions (s.4; also see Bridge et al (n 110 above), 33-050).

<sup>54</sup> Graham Battersby, ‘Acquiring Title by Theft’ (2002) 65(4) MLR 603, 610.

<sup>55</sup> Martin Dockray, ‘Why do we need Adverse Possession?’ [1985] Conv 272.

<sup>56</sup> Rostill (n 13 above), 144-154.

<sup>57</sup> *ibid*, 151-154.

<sup>58</sup> See e.g. Harold Demsetz, ‘Toward a Theory of Property Rights’ (1967) 57 Am Econ Rev 347, 356-358.

asset that is analogous to that of physical assets. Specifically, this limitation provision would be one where title to a digital asset would be extinguished after a number of years from the date at which a cause of action accrues.<sup>59</sup> It is difficult to imagine a similar limitation period not existing in the context of digital assets,<sup>60</sup> and so if there is such a provision, a new title<sup>61</sup> would need to be created in order to avoid a “proprietary vacuum”<sup>62</sup> and the negative consequences of such digital assets being underutilised. A new title<sup>63</sup> (and thus *a fortiori* a new property right) would also be needed to ensure that the extinction of title rules can properly perform their functions of providing certainty as to people’s rights as well as discouraging people from sitting on their rights. This new title would promote the efficient use of resources, and minimise the risk of a free-for-all.

### ***2.2.3 Conventions and expectations***

Furthermore, Crawford has another explanation/justification for the title in the physical asset context, namely the ‘expressive’ explanation.<sup>64</sup> According to this explanation, the ‘first possession’ rule arose as a convention governing claim-staking, and the convention was that whoever had the necessary degree of physical control accepted by society as a legitimate claim-staking act (coupled with an intention to stake a claim to the asset) would acquire title to the asset.<sup>65</sup> Crawford argues that the convention arose spontaneously as a result of natural psychological reasons – reasons that allow humans to be able to identify what other humans

---

<sup>59</sup> The Limitation Act does not have such a provision, and it is not possible to interpret any of the sections of the Limitation Act in a way that covers digital assets. For example, section 2 assumes the existence of a tort (and there is no specific tort that protects digital assets), and section 3 concerns conversion (which does not apply to digital assets).

<sup>60</sup> It is difficult to imagine such legislation not being passed in the future.

<sup>61</sup> Or at least a new property right plus the power to transfer it.

<sup>62</sup> See Battersby (n 54 above).

<sup>63</sup> Or at least a new property right plus the power to transfer it.

<sup>64</sup> Crawford (n 18 above), chapter 3.

<sup>65</sup> *ibid*, 77-79.

would consider ‘salient’.<sup>66</sup> According to Thomas Schelling, humans have a very good idea of what others would consider a ‘salient’ characteristic that allows them to coordinate conduct in the absence of communication (in this case, physical control).<sup>67</sup>

Crawford argues that this spontaneously emergent convention is justified, and there are two steps in his reasoning. First, the possession rule is simple to apply. Possession is an observable act and is discernible through social cues (in a way that people would have fair warning and can thus know how to comply with this simple rule).<sup>68</sup> Any other rule that is desert-based (e.g. ‘labour’-based formulations) or utility-based (e.g. ‘need’ based formulations) would be too complex to apply because there would be information costs, adjudication costs, and inherent subjectivity that may very well lead to violence or (at the very least) an excessive number of disputes. Second, it meets a minimum standard of fairness because it does not systematically discriminate against any class of persons.<sup>69</sup> In combination, the fact that it is simple to apply and meets a minimum standard of fairness means that in Crawford’s view, it is preferable to all other (e.g. desert-based or need-based) rules.<sup>70</sup>

In the digital asset context, it is suggested that conferring title on someone who has factual positive and negative control (and the associated intention) gives effect (at least in large part) to the expectation/convention that if someone has control of a digital asset then he has title to it.

Indeed, one of the core purposes of the blockchain is to allow people to store and move value in an efficient and safe way without the need for a central counterparty or intermediary, and this is achieved through creating ‘locked virtual spaces’ (addresses) over which people can

---

<sup>66</sup> *ibid*, 108-112.

<sup>67</sup> *ibid*, 108-109, citing Thomas C Schelling, *The Strategy of Conflict* (Harvard University Press, 1960), 54-57 and 98.

<sup>68</sup> Crawford (n 18 above), chapters 4-5.

<sup>69</sup> *ibid*, chapter 5.

<sup>70</sup> *ibid*, chapter 5, especially at 131.

have exclusive control, and a ledger in which movements of assets between these ‘spaces’ are recorded.<sup>71</sup>

The creation of this ecosystem leads people to make assumptions, and the crucial assumption people make is that someone has control of one of these ‘spaces’ then he has (legal) title to assets in such a ‘space’. In other words, people make the general inference or assumption that when someone has control of a digital asset, he has title to it (the ‘control-title’ inference).<sup>72</sup> This also gains support from the strength of the ‘equivalent’ inference or assumption made in the physical asset context, namely that<sup>73</sup> a person with possession of a physical asset has title to it.

It is accepted (in the proof-of-work cryptocurrency context for example) that a miner’s act of mining the relevant cryptocurrency (which ends up in his public key) is a sufficient claim-staking act to acquire title.<sup>74</sup> This accords with the proposed threshold<sup>75</sup> because (1) the cryptocurrency in his public key indicates that he has exclusive control (since he has the private key), and (2) the intention to exercise exclusive control is apparent from the act of mining.<sup>76</sup>

If factual positive and negative control (i.e. having a digital asset at a person’s public address)<sup>77</sup> allows a person to obtain title, this tracks such an expectation in the case of a ‘first degree’ or ‘best’ title. Even in the case of a thief who executes an on-chain transfer of a cryptocurrency to his own public address (and thereby obtains a relative title), this still tracks

---

<sup>71</sup> ‘Transferring legal title to a digital asset’ (2023) 5 JIBFL 317, 317.

<sup>72</sup> There is of course the question of what degree of control triggers the control-title inference. The core case is where the person has the only key in a single-signature address, or all the keys in a multi-signature address. If there is a lower degree of control (e.g. having positive and/or negative control without having all the keys), some might make the control-title inference but others would not. Whether a person does so also depends on how the blockchain protocol is configured or programmed, as various protocols do not reveal whether an address is a single-signature or a multi-signature address.

<sup>73</sup> Liu, ‘Transferring legal title’ (n 71 above), 319.

<sup>74</sup> This is generally accepted by the crypto community, and in my personal experiences and dealings with market and industry participants.

<sup>75</sup> See Sections 2.1.1 and 2.1.2 above.

<sup>76</sup> See Section 2.1.1 and 2.1.2 above.

<sup>77</sup> Coupled with the relevant intention.

the market expectation to the extent that the thief has *some* title to the cryptocurrency.<sup>78</sup> This aligns with the position as far as physical assets are concerned since someone with a second-degree relative title to (and possession of) a physical good signals to the world, as a matter of convention or expectation, that he has a title, which can be (e.g.) alienated by way of sale.

The threshold makes sense in terms of the ‘notice’ or ‘fair warning’ function. If one has factual control of the assets in a public key (by having the private key), the fact that the assets are in a public key gives notice to the world that the asset is in someone’s exclusive control, and thus gives rise to the expectation that the asset is not unowned: this provides certainty for third parties who may want to interact with the asset. If the notice function is to be taken seriously, then it is the outward signs that should matter, instead of any private arrangement between the claimant and another party (as would be the case where the claimant has legal but not factual control). Indeed, the courts’ general reluctance in property to allow private arrangements between (e.g.) two people to give rise to duties on the part of third parties is based in large part on fair warning and information costs concerns (as would, for example, be apparent in *numerus clausus* cases such as *Hill v Tupper*<sup>79</sup> and *Keppell v Bailey*<sup>80</sup>).<sup>81</sup>

Also, the rule provides a sufficient degree of certainty for a party obtaining title since he will know that he obtains title when the asset appears in his public address and there are a number of confirmations.<sup>82</sup> In this sense, it is also a relatively simple rule to apply.<sup>83</sup>

---

<sup>78</sup> If there is a general ‘take free’ rule for *bona fide* purchasers (as with money and negotiable instruments), then will be a better ‘tracking’ of the expectation since a subsequent purchaser would take free of better titles.

<sup>79</sup> (1863) 2 H & C 121, 159 ER 51.

<sup>80</sup> (1834) 2 My & K 517, 47 ER 106.

<sup>81</sup> See also Ben McFarlane, ‘Keppell v Bailey (1834); Hill v Tupper (1863): The Numerus Clausus and the Common Law’ in Nigel Gravells (ed), *Landmark Cases in Land Law* (Hart Publishing, 2013) 1.

<sup>82</sup> The exact number of confirmations required would depend on the individual blockchain in question (and conventions/market expectations), but this is the same type of uncertainty that is tolerated in the physical asset context. Most people will rely on block explorers such as Etherscan for block information.

<sup>83</sup> It is also fair in the sense that it does not systematically discriminate against any class of persons: e.g. anyone can execute the relevant operations on a blockchain and obtain title to a new asset. See also Richard A Epstein, ‘Possession as the Root of Title’ (1979) 13 Georgia L Rev 1221.

#### ***2.2.4 Other ‘general’ justifications***

The proposed threshold for digital assets is also consistent with other ‘general’ justifications for property rights in the physical asset context. For example, one justification for property rights is that a person who has control of an asset can make best use of it, and conferring a property right on such person limits the need for this person to take defensive measures to safeguard the asset, thus ‘internalising’ potential ‘externalities’ that prevent the best use of such an asset.<sup>84</sup> Although the assumption behind this rationale can be questioned (because it is often the case that a person in control of an asset is not in the best position to maximise the use of the asset), the rationale itself applies to the same extent to digital assets. This is because insofar as we want to ‘internalise externalities’ and make sure the person who is in control of the asset is in the best position to make use of it, this applies in equal measure to digital assets. The threshold for digital assets is in line with this rationale, since a public address owner has positive and negative control of the asset(s) inside it and is (on this analysis) in the best position to use the asset.

Another justification for property rights is that they are necessary for a person to fully express and develop his personality, and in this regard, a person who has positive and negative control of a digital asset with the intention of exercising such control would be able to develop and give expression to his personality and identity.<sup>85</sup> Owning a digital asset in this way can be part of one’s self-expression, because digital assets can be symbols of affiliation as well as status. Owning (for example) a Bored Ape NFT allows one to have access to exclusive Discord chats for Bored Ape owners, and alienate the NFT by way of sale to realise its monetary value.

---

<sup>84</sup> Demsetz (n 58 above), 354-358.

<sup>85</sup> GWF Hegel, *The Philosophy of Right* (OUP, 1967) paras 41-71.

This sense of exclusivity and freedom to alienate can (and often does) become a core part of one's identity or personality.

It may be objected that although these justifications can be seen as consistent with the rule proposed, they can also justify a different rule. For example, the 'internalisation of externalities' justification can justify a rule other than the possession rule: it can be argued that in certain circumstances, collective ownership (instead of individual ownership obtained through possession) can provide the best use of a resource.<sup>86</sup> Nonetheless, this is the case for both physical and digital assets, so no additional problems arise specifically in the digital asset context as far as this is concerned. The possession/control rule may not provide the *optimal* allocation of resources from an efficiency perspective but at least it gives effect to general efficiency and externalities considerations to a significant extent. It is in the very nature of these 'general' justifications that they can be interpreted in various ways, and so they are consistent with a wide range of rules.

As the justifications for acquiring an original title to a physical asset apply to digital assets, it is suggested that the normative threshold of exclusive factual control (factual positive and negative control) should also apply in the digital asset context.

### ***2.2.5 Specific v general intention***

There is the question of whether the 'intention' requirement should be relaxed, to allow someone to obtain title to a digital asset in an address that he controls if he has a general intention to exercise control over assets that come into the address, even though he does not know about the specific digital asset.

---

<sup>86</sup> See e.g. Robert Ellickson, 'Property in Land' (1993) 102 Yale LJ 1315, 1332-1344.

This type of ‘general’ intention requirement that does not require an intention in relation to a *specific* asset is an exception to the general rule that the intention must exist in respect of the specific asset. Nonetheless, the more relaxed ‘general’ intention requirement can be seen in the physical asset context, and a prime example is the *Parker* rule.<sup>87</sup> Under *Parker*, if one intends to exercise control over chattels that are found in his building generally, he would acquire title to such chattels even though he does not specifically know of their existence.<sup>88</sup> This ‘general intention’ requirement is also seen in Article 11 of the DAL, where one acquires title if he has a general intention to exercise control over assets in an address.<sup>89</sup>

It is suggested that the arguments in favour of relaxing the requirement to that of ‘general intention’ are weak, and that the arguments against such a relaxation are much stronger. Thus, such a relaxation should not be made.

From C’s perspective, one of the main benefits of a ‘general intention’ requirement is that if C has control over an address and intends to exercise control over all assets that come into the address, and D misappropriates an asset airdropped into the address which C does not know about at the time of the misappropriation, C can sue D for interference. This situation would exist for example where X mints an asset into C’s address (by way of an airdrop gift), and D misappropriates it before C knows about the asset (even though C has a general intention to exercise control over all assets in his address).

In this situation, C may have formed a general expectation that he can use the assets located in his address. However, this does not demonstrate that the absence of a remedy in this situation is unfair. As stated in Chapter 1, the core purpose of conferring a property right to a digital asset is to protect someone’s ability to use the asset. Thus, the law should only protect someone’s ability to use the asset (by conferring a property right) if he has a certain likelihood

---

<sup>87</sup> *Parker v British Airways Board* [1982] 1 QB 1004.

<sup>88</sup> *ibid*, 1019-1020.

<sup>89</sup> DAL, Article 11(1).

of using the asset. Thus, if someone (C) is not even aware of the existence of a digital asset that has been (e.g.) airdropped into an address he controls, there is a much lower likelihood of him using the asset at any point in time, as compared to the situation where he has knowledge of the specific asset and intends to exercise control over it.

Also, C's lack of knowledge of the specific asset means he has not formed an expectation that he would be able to exercise the transactional powers associated with the specific asset. A 'general' expectation that one is able to exercise the transactional powers in relation to assets that come into the address (that one may not currently know about) is much more diffuse than an expectation that one is able to exercise the transactional powers associated with a specific asset that one knows is in the address (which is a much more crystallised and precise expectation). Defeating the former expectation is much less intrusive than defeating the latter expectation.<sup>90</sup>

In addition, the 'conventions and expectations' justification mentioned in Section 2.2.3 above does not apply to a situation where there is no intention to exercise control over the (specific) asset in question. Crawford's justification for property rights arising via possession is based on a person communicating his intention to stake a claim over the asset, via acts that function as recognised signals about such an intention.<sup>91</sup> Without an intention to exercise control over the specific asset, there is no intention to stake a claim in respect of it. Thus, Crawford's 'conventions and expectations' justification only supports a 'specific intention' requirement – it does not support a 'general intention' requirement.

---

<sup>90</sup> Linking this back to Bentham's 'expectations' justification of property rights, he notes that "Property is nothing more than the basis of a certain expectation; namely, the expectation of deriving hereafter certain advantages from a thing (which we are already said to possess) by reason of the relation in which we stand towards it" (Jeremy Bentham, *The Theory of Legislation* (London, 1802), 145). It is suggested that where C has knowledge of the relevant asset (and an intention to exercise control over it), the expectation of deriving advantages from that asset is much more crystallised, compared to where there is no knowledge of the relevant asset.

<sup>91</sup> Crawford (n 18 above), 60, 63.

Nonetheless, proponents of a general intention requirement may argue that assets in a public address are somewhat analogous to assets on a piece of land, because just like the former, the latter often involves a ‘locked space’ in which assets can be located. Thus, if the justifications for the *Parker* rule are convincing, then they may well also justify a general intention requirement in the digital asset context.

However, the justifications for the *Parker* rule have been criticised,<sup>92</sup> for good reason. For example, insofar as the *Parker* rule is justified on the basis that it functions as an evidential presumption that the person who intends to exercise control of the chattels on his land intends to exercise control over the specific chattel in question,<sup>93</sup> this is simply not the case. This is because, as noted by Crawford, there is simply no room to rebut such a presumption, as demonstrated in *National Crime Authority v Flack*.<sup>94</sup> In *Flack*, the claimant did not know there was a briefcase containing cash<sup>95</sup> that was in her house, yet obtained title to the briefcase and cash.<sup>96</sup> This result would be impossible if the ‘presumption’ view were correct, because the claimant’s lack of knowledge of the briefcase (and the cash inside it) would have rebutted any presumption of intention. Similarly, insofar as the *Parker* rule is justified on the basis that the occupier’s intention to exercise control over the chattel in question is not express but manifest<sup>97</sup> (when the occupier intends to exercise control over the chattels on his land), this justification is inconsistent with the result in *Flack* where there was no such intention yet the claimant obtained title to the chattels.<sup>98</sup>

Indeed, where the justifications for the *Parker* rule are unconvincing, the case for a general intention requirement in the digital asset context would be much weaker.

---

<sup>92</sup> See e.g. Crawford (n 18 above), 154-157.

<sup>93</sup> *ibid*, 155, discussing Hickey’s ‘presumption’ view (Robin Hickey, *Property and the Law of Finders* (Hart Publishing, 2010), 46-47 and 52.

<sup>94</sup> *Chairman, National Crime Authority v Flack* [1998] FCA 932; (1998) 86 FCR 16.

<sup>95</sup> Specifically 433,000 AUD in bank notes.

<sup>96</sup> *Flack* (n 94 above), 25-27.

<sup>97</sup> See discussion at Crawford (n 18 above), 155.

<sup>98</sup> See also Hickey (n 93 above), 46-53 (discussion and criticism of the *Parker* rule).

Thus, it is suggested that the specific intention requirement should be maintained, because the arguments in favour of relaxing the requirement to that of ‘general intention’ are much weaker than the arguments against such a relaxation.

### **3. The doctrinal question: possession or control?**

Having clarified the general normative threshold for acquiring an original title to a digital asset, the follow-up question is how to analyse this as a matter of doctrine. Specifically, should we assimilate this rule within the general doctrine of possession, or should we use the concept of control?

At the moment, possession is a doctrine that only applies to physical assets.<sup>99</sup> If it were to be extended into the digital asset sphere, it would straightforwardly cover the situations described above, and would be able to govern the question of acquiring title to a digital asset.

It would also mean that all possession-dependent doctrines would presumptively apply to digital assets. This is because (in English law generally), people attach consequences when a particular legal concept or label is used. In this case, if a digital asset is capable of being possessed (i.e. the ‘possession’ label applies to digital assets), people will attach consequences to such a characterisation. Specifically, possession of an asset (when combined with other circumstances/features) would presumptively be sufficient to create particular legal relationships (such as bailment) or allow someone to sue in tort for interfering with the asset. The doctrines of bailment, conversion, trespass, reversionary injury, pledges and liens etc would presumptively apply to digital assets.

Indeed, some may say this is useful because we are importing existing doctrines instead of starting from scratch, in a way that useful protection can be provided to parties who transact

---

<sup>99</sup> See e.g. *OBG v Allan* [2007] UKHL 21 and *Your Response v Datateam* [2014] EWCA Civ 281.

and deal with digital assets (e.g. in the tortious interference context). This point has been made in the academic literature as well as by the Law Commission.<sup>100</sup>

However, it is argued in this section that (1) such an extension should not be made, and (2) the concept of ‘control’ should be used instead.

My first claim that ‘possession’ should not be applied to digital assets consists of four arguments. First, the possession rules are messy and unsatisfactory even as applied to physical assets, and so extending such rules to digital assets would replicate the mistakes made in the context of physical assets. Second, there are many differences between physical and digital assets, meaning that possession (as a doctrine specifically designed for physical assets) is a bad fit for digital assets, which creates a very significant risk of wrong analogies and random decisions.<sup>101</sup> Third, accepting that digital assets can be possessed means that every possession-dependent doctrine would presumptively apply to digital assets, and it would as a result be difficult to argue that a normal consequence of possession should *not* apply to digital assets even if such a consequence is normatively undesirable (because of the natural path-dependence of extending a concept to cover a new type of object or asset). Fourth, applying possession to digital assets creates undesirable practical consequences in the litigation context.

After establishing that ‘possession’ is an undesirable concept, I will then argue that ‘control’ is the preferable concept to apply in the context of digital assets. It applies to all kinds of property, and its meaning can be clarified in the digital asset context, and so the negative consequences in respect of ‘possession’ can be avoided. In particular, there is no need to deal

---

<sup>100</sup> See e.g. Law Commission, *Electronic trade documents* (n 18 above), 3.26, 5.22, 5.25, 8.17; Law Commission of England and Wales, ‘Digital assets: electronic trade documents – A consultation paper’ (CP 254, 30 April 2021), 5.85, 6.103-6.110; Sarah Green and Ferdisha Snagg, ‘Intermediated Securities and Distributed Ledger Technology’, in Louise Gullifer and Jennifer Payne (eds), *Intermediation and Beyond* (Hart Publishing, 2019) 337, 345-348.

<sup>101</sup> ‘Control’ matches with the substance of the (normative) threshold described in Section 2.1. It fits better than possession (as it is the ‘common ingredient’ of the two: see text to nn 249-250 below).

with the need to reconcile a doctrine designed for physical assets with the idiosyncrasies of digital assets.

This section will be structured as follows. I will first explain the concept of possession and how it has been applied in English law, as well as its role in giving rise to a ‘general property interest’. I will then make the claim that extending possession to digital assets is undesirable, and go through the four arguments outlined above in turn. Finally, I will explain the concept of control and argue that it is the preferable concept to apply in the digital asset context.

### **3.1 Possession and its context**

It is useful to begin by exploring the concept of possession, and how it has been used in English law. In the context of acquiring an original title to an asset, possession involves exercising exclusive physical control over a (physical) asset, with the intention of exercising it on one’s own behalf

This can be seen in *Powell v McFarlane*, where Slade J held that possession (for the purposes of acquiring title) requires “factual possession and the requisite intention to possess”.<sup>102</sup> Slade J was cited in *Pye v Graham*,<sup>103</sup> where Lord Browne-Wilkinson further summarised and explained the requirements for possession, namely “a sufficient degree of physical custody and control”, and “an intention to exercise such custody and control on one’s own behalf and for one’s benefit”.<sup>104</sup> There is no requirement for the claimant to intend to *own* the property.<sup>105</sup>

---

<sup>102</sup> (1977) 38 P & CR 452, 470.

<sup>103</sup> [2002] UKHL 30, [2003] 1 AC 419.

<sup>104</sup> *ibid.*, [40].

<sup>105</sup> Mirroring the discussion at sections 2.1.1 and 2.1.2 above.

But ‘possession’ has been used in vastly different senses in other contexts. It has been used to refer to legal control (as opposed to factual control): for example a bailor has been said to be in ‘possession’ of an object even though he does not have factual control of it but merely has a right against the bailee to demand its return.<sup>106</sup> ‘Possession’ has also been used to refer to the satisfaction of conditions required for a person to be able to sue third parties for interference (in a way that does not involve factual control). For example, in *Wilson v Lombank*,<sup>107</sup> the plaintiff’s car was parked in a garage (over which he did not have factual possession or control). When the defendant took the car away, the plaintiff sued in trespass. Despite the lack of factual control over the car, the court held that the plaintiff had ‘possession’ of the car such that he was able to sue in trespass.<sup>108</sup> Similarly, the ‘right to immediate possession’ determines the outer boundaries of when a person has title to sue in the torts of conversion and negligence.<sup>109</sup> Factual possession of the object is not required.

In addition, the label ‘constructive possession’ has been used to refer to situations where one has possession of a paper document that ‘represents’ or ‘symbolises’ possession of goods, but does not have physical control of the goods. In such a situation, the holder of the document has certain rights that relate to the goods. For example, the holder of a bill of lading has a right against the carrier to the delivery of the asset,<sup>110</sup> and this is referred to as ‘constructive possession’.<sup>111</sup> If I hold a bill of lading representing wine that has been loaded onto a ship, the

---

<sup>106</sup> *Ancona v Rogers* (1876) 1 Ex D 285, 292.

<sup>107</sup> (1963) 1 WLR 1294.

<sup>108</sup> *ibid*, 1297-1298.

<sup>109</sup> See generally Section 3.2.1.2 below.

<sup>110</sup> A holder of a bill of lading can have neither title nor actual possession. Since the passing of property is determined by the intention of the parties, a bill of lading holder does not necessarily have title to the goods, e.g. if the intention of the parties is for title to pass only upon payment: Michael Bridge, *Benjamin’s Sale of Goods* (11<sup>th</sup> ed, Sweet & Maxwell 2020) 18-231. The core right embodied in a bill of lading is the right against the carrier to delivery of the goods, along with other rights against the carrier based on the contract of carriage (Michael Bridge, Louise Gullifer, Kelvin Low and Gerard McMeel, *The Law of Personal Property* (3<sup>rd</sup> edition, Sweet and Maxwell 2021), 5-030 and 5-031). The analogy between a holder of a bill of lading and a holder of a ‘key to floating warehouse’ (*Sanders Bros v Maclean & Co* (1883) 11 QBD 327, 341) is not sound because there is no sense in which the holder of the bill of lading has factual control over the goods (unlike the holder of an actual key).

<sup>111</sup> Bridge et al (n 110 above), 5-031.

bill of lading gives me a right to obtain possession of the wine once it has been delivered to the relevant destination. Furthermore, acts in relation to the paper ‘symbol’ of possession are also (in certain circumstances) considered to be equivalent to an act in respect of the underlying asset: e.g. pledging a bill of lading can operate as a pledge of the underlying goods.<sup>112</sup>

‘Possession’ has also been used to refer to the property interest that one obtains through taking possession: in *Watts v Stewart*,<sup>113</sup> the property right to exclude all others was referred to as “legal exclusive possession”.<sup>114</sup>

Also, even though ‘possession’ has been held not to apply to intangibles, judges have used the phrase ‘equitable possession’ in the context of intangible interests. This is apparent from *Dearle v Hall*,<sup>115</sup> where Sir Thomas Plumer referred to the act of giving notice to the trustee following an assignment of a beneficial interest as taking ‘equitable possession’ of the beneficial interest.<sup>116</sup>

‘Possession’ has also been used to denote a relationship between a person and a corporeal estate, as the term ‘possession of estates and interests’ is used to describe someone who either (1) has title to land, or (2) is factually enjoying the incidents of an estate in land.<sup>117</sup>

Finally, ‘possession’ is used in the context of criminal law, for example in the context of the ‘possession of controlled drugs’ offence under s.5 of the Misuse of Drugs Act 1971. Here, what is required is for the defendant to (1) have physical control of the ‘controlled drug’,<sup>118</sup> and (2) know that he has physical control of the object or ‘thing’ that is the drug.<sup>119</sup> The defendant does not need to know that the object is a controlled drug to be liable, but a lack

---

<sup>112</sup> This is the case if the bill is pledged to a mercantile agent: *Official Assignee of Madras v Mercantile Bank of India* [1935] AC 53; Factors Act 1889, s 3.

<sup>113</sup> [2016] EWCA Civ 1247.

<sup>114</sup> *ibid*, [31].

<sup>115</sup> (1828) 3 Russ 1.

<sup>116</sup> *ibid*, 12.

<sup>117</sup> Mark Wonnacott, *Possession of Land* (CUP 2006) ch 1, p 1-3 and 44; Rostill (n 13 above), 23-24.

<sup>118</sup> David Ormerod and David Perry (eds), *Blackstone’s Criminal Practice 2022* (OUP, 2021), B19.28; but also note Misuse of Drugs Act 1971, s.37(3): “For the purposes of this Act the things which a person has in his possession shall be taken to include any thing subject to his control which is in the custody of another”

<sup>119</sup> Ormerod and Perry (n 118 above), B19.29.

of knowledge that the object is a controlled drug may in certain circumstances constitute a defence.<sup>120</sup>

As such, it can be seen that the concept of ‘possession’ has been deployed in many contexts, some quite far removed from the case of exclusive physical control over an asset.<sup>121</sup> For the purposes of this chapter, the primary meaning of ‘possession’ that will be used is exclusive physical control of an asset (with the requisite intention to possess it), i.e. the conditions required to acquire an original title to a physical asset. Nonetheless, as will be seen, the moment we say that a digital asset can be possessed, other meanings of possession can be presumptively applicable – such as the ‘right to immediate possession’.

### ***3.1.1 Scope of ‘possession’***

The current law provides that possession (and its associated protections and advantages) is only applicable to tangible assets. This is clear from the cases of *Your Response v Datateam*<sup>122</sup> and *OBG v Allan*,<sup>123</sup> which will be explored.

In *Your Response*, the claimant magazine publisher and the defendant database manager were involved in a dispute concerning substandard work in respect of the management of subscription lists. The claimant purported to terminate the contract, and when the defendant sued for fees, the claimant counterclaimed for breach of contract. The defendant claimed a lien over the (intangible) database, and this did not succeed before the Court of Appeal. The court held that a lien could not arise over an intangible database, and Moore-Bick LJ noted that “[p]ossession is concerned with the physical control of tangible objects”.<sup>124</sup> As a lien requires

---

<sup>120</sup> Misuse of Drugs Act 1971, s.28; Ormerod and Perry (n 118 above), B19.105.

<sup>121</sup> Coupled with the intention to exercise exclusive physical control over the asset.

<sup>122</sup> *Your Response v Datateam* [2014] EWCA Civ 281, [2015] QB 41.

<sup>123</sup> *OBG Ltd v Allan* [2007] UKHL 21, [2008] 1 AC 1.

<sup>124</sup> *Your Response*, (n 122 above), [23].

possession, it cannot extend to a non-possessable object such as an intangible database. The concept of ‘possession’ was distinguished from ‘practical control’.<sup>125</sup> Practical control is a much wider concept, as it can apply to intangible objects, as well as “things which the law would not regard as property at all”.<sup>126</sup> ‘Possession’ is a narrower concept, only applicable to tangibles.

In *OBG v Allan*, the claimant’s creditors invalidly appointed receivers, who took control of the claimant’s assets, dealing with the claimant’s chattels as well as purporting to settle its debts and terminate its contracts. The defendant sold the claimant’s chattels without the latter’s authority, and the latter’s debts were settled for ‘less...than would have been obtained in an orderly winding up’.<sup>127</sup> The claimant brought a claim in conversion in respect of both the chattels and the debts. While liability in respect of the chattels was accepted, the claim in respect of the debts failed. By a 3-2 majority, the House of Lords declined to extend the tort of conversion to intangible assets. As Lord Brown noted, granting the full claim would involve “the...severance of any link whatever between the tort of conversion and the wrongful taking of physical possession of property (whether a chattel or document) having a real and ascertainable value”.<sup>128</sup> In other words, since conversion is a tort that protects people against interferences with possession, it can only apply to assets that can be possessed (i.e. tangible goods). Intangibles cannot be converted, since they cannot be possessed and so there is no ‘possession’ that can be infringed. This was reiterated in *Your Response*: “As *OBG v Allan* makes clear, the essence of conversion is a wrongful interference with the possession of tangible property...In contrast to chattels, choses in action are intangible things and incapable of the physical possession necessary to support a claim for conversion.”<sup>129</sup>

---

<sup>125</sup> *ibid*, [23].

<sup>126</sup> *ibid*, [23].

<sup>127</sup> *OBG* (n 123 above), [311].

<sup>128</sup> *ibid*, [321].

<sup>129</sup> *Your Response* (n 122 above), [15].

Furthermore, as Lord Hoffmann noted in *OBG*, extending the tort of conversion to intangible choses in action would cut across the regime that governs pure economic loss (where recovery is “limited” (in the case of negligence) or there is a specific mental element (in the case of the economic torts)). It would effectively impose “strict liability for pure economic loss” on people who act in “good faith”.<sup>130</sup> The situation involving ‘documentary intangibles’ such as cheques (where conversion is allowed) was distinguished from ‘pure’ intangibles such as debts, since in the former case there remains a physical document on which the tort of conversion could nonetheless still fasten.<sup>131</sup>

This means that the ‘possession’ concept does not apply in the digital asset context because digital assets are intangible. Yet, many digital assets (like physical assets) are capable of being reduced to someone’s exclusive control, and can be transferred from person to person.<sup>132</sup> It might be argued, therefore, that the ‘possession’ regime should extend into the digital asset context, so that the same legal consequences (e.g. the entitlement to sue third parties for interference with the asset under the ‘chattel torts’) would attach. Without these consequences, individuals would be prejudiced as (for example) they would not be able to sue a third party who destroys or damages a digital asset, since in order to be able to sue in (e.g.) conversion, the asset damaged must be capable of being possessed. Individuals would also be prevented from creating bailment relationships and possessory security, which may well be detrimental to commercial flexibility. This argument will, however, be rejected in Section 3.2 below.

### ***3.1.2 The ‘general property interest’***

---

<sup>130</sup> *OBG* (n 123 above), [99].

<sup>131</sup> See e.g. *ibid*, [321]. Also see *Your Response* (n 122 above), [15]: “Even in the case of the conversion of valuable documents (cheques etc.), to which several of their Lordships referred, there is an unlawful interference with a physical object to which a commercial value can be attached”.

<sup>132</sup> See section 2.1 above and Hin Liu, ‘The Legal Nature of Blockchain Securities’ [2021] LMCLQ 476, 484.

As mentioned earlier,<sup>133</sup> taking possession of an asset<sup>134</sup> confers on the possessor a ‘general property interest’.<sup>135</sup> This proprietary right entitles the possessor to sue third parties for interference, and also confers certain powers on the possessor, such as the power to transfer title to the asset, and the power to create derivative interests (such as security interests).<sup>136</sup> This right however, is subject to better titles (e.g. if the possessor is not the true owner, his ‘general property interest’ is not enforceable against the true owner). In this sense, the possessor’s title can be understood as being ‘relative’.

It is also important to note that although taking possession is required to give rise to a general property interest, one need not be in possession of the relevant asset to retain the right to sue for wrongdoing: in other words, the right is not possession-dependent. For example, in *Costello*,<sup>137</sup> the defendant committed conversion despite the claimant not being in (factual) possession at the time of the acts constituting the wrong (retaining the vehicle past the period authorised by statute). Also, even if the possessor is not the true owner (e.g. if he is a thief), he is entitled to sue third parties for interference.<sup>138</sup>

Another point to note is that a general property interest does not *confer* a liberty to use the asset. There is no change in the legal position as far as liberties are concerned, because even before taking possession, a person has a liberty to use a particular asset vis-à-vis the world (if there are no pre-existing superior titles). Even if there are pre-existing superior title(s), taking possession (and gaining a general property interest) does not change the position, since the

---

<sup>133</sup> See section 2.2 above.

<sup>134</sup> In the sense of having factual possession and an intention to possess.

<sup>135</sup> *Armory v Delamirie* [1722] EWHC KB J94; *Costello* (n 42 above). Luke Rostill calls this a ‘general property interest’: see Rostill (n 13 above), 112-113, Rostill, ‘Terminology and title to chattels’ (n 15 above).

<sup>136</sup> Rostill (n 13 above), 112. The key features of a general property interest are the right to exclude the world from the asset (apart from people with a better title) that is not possession-dependent, and a power to transfer the interest to another person.

<sup>137</sup> *Costello* (n 42 above); also see Rostill, ‘Terminology and title to chattels’ (n 15 above), 414 (title not possession-dependent).

<sup>138</sup> *Bridge et al* (n 110 above), 33-035; See *Jeffries v Great Western Railway Co* (1856) 5 E&B 802, 806, 119 ER 680; *Costello* (n 42 above).

liberty was (and is still) subject to a duty vis-à-vis the people with superior title(s), regardless of whether one takes possession of the object. What is crucial is that *other people* will be under a duty not to interfere with the relevant physical object when one takes possession of the object.<sup>139</sup>

### **3.2 Possession should not be extended to digital assets**

Having set out the context behind the ‘possession’ concept, I will now argue that the concept of possession should not be extended to digital assets. The four arguments for why this is the case (outlined in Section 3)<sup>140</sup> will be explored in turn.

#### ***3.2.1 The possession rules are messy/unsatisfactory***

It is suggested that the possession jurisprudence is messy and unsatisfactory even in the physical asset context, and such difficulties should not be carried over into the digital asset context. Two examples will be given here.

##### **3.2.1.1 Bailment**

The first example concerns the doctrine of bailment. Bailment is essentially a relationship between a ‘bailor’ and ‘bailee’ where the bailee consents to holding the bailor’s good(s), and this requires the bailee to come into possession of a physical asset. Although bailment is a

---

<sup>139</sup> Simon Douglas and Ben McFarlane, ‘Defining Property Rights’ in Penner and Smith (eds), *Philosophical Foundations of Property Law* (Oxford, 2013) 219, especially 219-222.

<sup>140</sup> See Section 3, para 6 above.

contextual legal category<sup>141</sup> just like (e.g.) ‘sale’, it has been treated as a source of rights/obligations.<sup>142</sup> As McMeel argues however, treating bailment as a distinct source of obligations is redundant and liable to confuse because the content of bailment law can just be subsumed under the existing categories of contract, tort, unjust enrichment and property.<sup>143</sup>

For example, a bailee’s duty of care results from consent, which in both the tort and contract context is a reason for imposing obligations. If consent (plus physical proximity in the form of possession) is sufficient to give rise to a duty of care, this is explicable by reference to tort principles without needing to resort to a separate concept of bailment.<sup>144</sup> Specifically, the assumption of responsibility principle is relevant. Bailment essentially consists of a duty of care in respect of a chattel that arises from an assumption of responsibility by the bailee to the bailor, as the bailee is ‘taking on a task’<sup>145</sup> for the bailor.<sup>146</sup> The standard of care of a bailee in a particular case is often (or usually) different from that in respect of the general duty to take reasonable care not to damage chattels,<sup>147</sup> but this does not take bailment outside the realm of duties of care (and tort law):<sup>148</sup> even in other contexts (such as medical negligence), the standard of care is varied according to the circumstances.<sup>149</sup> The label of ‘bailment’ obscures these aspects, hides the core normative issues, and compromises the transparency of the courts’ reasoning.

---

<sup>141</sup> Gerard McMeel, ‘The redundancy of bailment’ [2003] LMCLQ 169, 175-177.

<sup>142</sup> E.g. *Yearworth v North Bristol NHS Trust* [2009] EWCA Civ 37 [2010] QB 1; *The Pioneer Container* [1994] 2 AC 324, 339, 342 (Lord Goff) .

<sup>143</sup> McMeel (n 141 above), 169-171, 199-200.

<sup>144</sup> The bailee’s duty of care is tailored to the specific context of safeguarding goods, but it remains a duty of care nonetheless. See e.g. *Bridge et al* (n 110 above), 12-030-12-037.

<sup>145</sup> Donal Nolan, ‘Assumption of Responsibility: Four Questions’ (2019) 72 CLP 123, 133-135.

<sup>146</sup> *Ibid*, 130.

<sup>147</sup> See e.g. *ibid*, 138; Andrew Burrows (ed), *English Private Law* (3rd ed, OUP 2013) para 16.36; *Bridge et al* (n 110 above), 12-034 and 12-035.

<sup>148</sup> *Bridge et al* (n 110 above), 12-030: “bailees, whether acting under contract, or acting gratuitously, owe a duty of care to take reasonable care of the goods such as is required by the circumstances of the particular case.”

<sup>149</sup> See e.g. *Bolam v Friern Hospital Management Committee* [1957] 1 WLR 582 (medical negligence: the standard of care is satisfied as long as the defendant’s conduct meets the standard of a responsible body of medical opinion, though this principle does not apply in informed consent cases: *Montgomery v Lanarkshire Health Board* [2015] UKSC 11); *Maynard v West Midlands RHA* [1984] 1 WLR 634.

The use of ‘bailment’ to describe a duty of care arising from an assumption of responsibility can be seen in *Yearworth v North Bristol NHS Trust*.<sup>150</sup> The claim involved mishandling of sperm by the defendant hospital, and the defendant admitted that it had a duty of care and breached its duty to the claimant in respect of the sperm.<sup>151</sup> The court stated that there was an additional cause of action in bailment, separate from tort. However, it is noteworthy that the bailment duty was analysed in terms of an assumption of responsibility: “The unit’s assumption of responsibility for the careful storage of the sperm was express and unequivocal: ‘we can undertake to look after [it] with all possible care’”.<sup>152</sup> This ‘voluntary assumption of responsibility’ analysis falls squarely within the territory of tort law (and duties of care), as the defendant undertook to take on the task of storing the claimant’s sperm with care. The ‘bailment’ label may lead to a mistaken emphasis on how the defendant “chose to take possession”<sup>153</sup> of the sperm or how it “held itself out...as able to deploy special skill”<sup>154</sup> without connecting these factors to the normative reason for generating the obligation. It should not be seen as a source of obligations distinct from tort, contract or unjust enrichment, because it is not. Misleadingly framing it as such would act either as a distraction that hides the core normative issue (as in *Yearworth* itself) and/or a shortcut that obscures the underlying reasoning.

Bailment can also be used as a substitute for contractual reasoning, as can be seen in *The Pioneer Container*.<sup>155</sup> This involved a contractual claim by a head bailor against a sub-bailee in respect of goods that were lost due to a sinking ship. The issue was whether the head bailor was bound by an exclusive jurisdiction clause between the head bailee and the sub-bailee of which it was unaware. The court held that it was so bound, on the basis that the head bailor

---

<sup>150</sup> *Yearworth* (n 142 above).

<sup>151</sup> *ibid*, [13].

<sup>152</sup> *ibid*, [49(a)].

<sup>153</sup> *ibid*, [49(d)].

<sup>154</sup> *ibid*, [49(d)].

<sup>155</sup> *Pioneer Container* (n 142 above).

had authorised the head bailee to make sub-bailments (that may affect the legal position of the head bailor). Lord Goff stated that this result comes from the law of bailment, not the law of contract: “it does not depend for its efficacy either on the doctrine of privity of contract or the doctrine of consideration”.<sup>156</sup> However, this hides the fact that the normative basis of the conclusion derives from a need to have an exception to the privity rule.<sup>157</sup> Indeed, there seems to be a wider principle in play, namely that an exception to the privity of contract rule applies where A has authorised B to enter into a sub-contract that may contain terms affecting A’s legal position (in which case A would be bound by such terms). If this is so, such a principle should not be confined to the bailment or chattels context.<sup>158</sup>

Furthermore, bailment does not explain why a bailee has title to sue for interference torts: since it is the bailee’s *possession* that allows him to sue, it is the law of property that explains this feature. Bailment, just like sale, is a label to describe a *contextual* occasion whereby a particular set of duties (e.g. a duty of care) is typically imposed.<sup>159</sup>

Applying the bailment doctrine to digital assets<sup>160</sup> means that the same mistake of mischaracterising bailment (as a source of obligations as opposed to a contextual category) is liable to occur. This could lead to poorly reasoned decisions where the bailment doctrine is engaged. If ‘bailment’ is a sufficient explanation for granting particular rights or duties in the digital asset context, judges would not need to explicitly state the normative reason for conferring such rights or duties. In other words, judges may themselves be misled into thinking that bailment is a distinct normative source of obligations (and present it as such), and thus would not necessarily have to justify their decisions with transparent and rigorous reasoning

---

<sup>156</sup> *ibid*, 339.

<sup>157</sup> Specifically, an exception to the ‘burden’ part of the privity rule, such that liabilities are imposed on person(s) who are not party to the contract.

<sup>158</sup> McMeel (n 141 above), 197-198. Indeed, the exception should not be possession dependent.

<sup>159</sup> *ibid*, 175-177.

<sup>160</sup> If a digital asset can be possessed, it can presumably be bailed because there can be a transfer of possession of a digital asset: see Hin Liu, Louise Gullifer and Henry Chong, ‘Client-intermediary relations in the crypto-asset world’ in Paul Davies and Tan Cheng-Han (eds), *Intermediaries in Commercial Law* (Hart Publishing, 2022) 213, Section II.C.

with reference to the actual normative reasons for imposing such obligations.<sup>161</sup> This, then, creates a risk of courts obscuring the true basis for their decisions, and potentially creating incoherence in the law.<sup>162</sup>

In any event, bailment will serve as a redundant distraction from the main issues at stake in scenarios that involve digital assets. Where a digital asset is held by an exchange for example, the incidents of bailment can be replicated by contract and trust,<sup>163</sup> and so it is unnecessary to add the extra ‘bailment’ label.

### 3.2.1.2 The ‘right to immediate possession’

Second, the concept of a ‘right to immediate possession’ is unsatisfactory. This concept governs the boundaries for when a person has title to sue in conversion, and the current legal position is that a person who has title to an asset may not have the ‘right to immediate possession’, and thus may not be able to sue in conversion. In particular, a bailor (lessor) in a chattel lease does not have the right to sue for conversion.<sup>164</sup> It will be argued here that this assumption that a party with a property right can lose general protection from interference if he loses a ‘right to immediate possession’ is incorrect, and should not be carried over into the digital asset context. The true position, it will be argued, is that a person with title only loses the right to sue for interference when he has granted a derivative legal property right (and not where he has simply given another party a personal right).<sup>165</sup> In relation to goods, the concept

---

<sup>161</sup> In *The Pioneer Container* (n 142 above), Lord Goff held that the sub-bailee comes under a duty to the bailor that “finding its origin in the law of bailment rather than the law of contract, does not depend for its efficacy either on the doctrine of privity of contract or on the doctrine of consideration” (339). See also 342.

<sup>162</sup> In the *Pioneer Container* context, the threshold arguably disrupted is that in relation to privity of contract.

<sup>163</sup> Liu, Gullifer and Chong (n 160 above), Section IV.

<sup>164</sup> *Gordon v Harper* (1796) 7 TR 9, 101 ER 828.

<sup>165</sup> Given that the case law has not settled the question of whether a chattel lease is a property right. See e.g. Ben McFarlane’s stance that outside the land context, “the property law system does *not* recognise a property right equivalent to ‘exclusive control for a fixed period’” (emphasis added) and so it is “simply impossible...to divide Ownership...into separate, distinct slices of time: A must either transfer his Ownership to B *completely*

of ‘right to immediate possession’ has served as a distraction from the main issue: whether a derivative legal property right has been granted in respect of the (physical) asset in question. As a result, the underlying normative considerations have been obscured.

### 3.2.1.2.1 When the right to sue is lost

In general, in both the land and the chattels context, a person who has title does not lose the right to sue for interference unless a derivative legal property right is granted,<sup>166</sup> the effect of which is to ‘fragment’ his title and confer a right to sue on the derivative interest-holder.<sup>167</sup> This is because the default position is that a person with title has the right to exclude,<sup>168</sup> which entails the immediate right to possess the land or good(s) and thus sue third parties for interference (given that such right is one of the core incidents of a property right). Thus, one can only lose the right to sue<sup>169</sup> if the right to possess/exclude (which is exigible against the world) has been given to another person through the grant of a derivative property interest. In this situation, the grantor of the derivative interest can only sue for damage to his residual or ‘reversionary’ interest. The concept of ‘reversionary injury’ deals with the situation where there is damage to the owner’s reversionary interest<sup>170</sup> (which in turn assumes that derivative interests can be granted).

In the chattels context, a pledge involves the granting of a derivative interest to the pledgee, under which the pledgor cannot demand the return of the asset until the underlying

---

or not at all”: Ben McFarlane, *The Structure of Property Law* (Hart Publishing, 2008), 148-149. On his view therefore, a chattel lease is not a derivative interest (see discussion at 149-150).

<sup>166</sup> E.g. a lease (in the land context) or a pledge (in the chattels context).

<sup>167</sup> E.g. where a (legal) lease has been granted over the lessor’s freehold.

<sup>168</sup> McFarlane (n 165 above), 140-146 (ownership as a right to exclusive control forever).

<sup>169</sup> In situations where there is not the sort of damage that would form the basis of a claim for damage to a reversionary interest.

<sup>170</sup> I.e. where the relevant damage concerns the (future) period in which the owner is entitled to immediate possession.

obligation has been performed.<sup>171</sup> Here, the pledgor cannot sue third parties for conversion, but the pledgee can.<sup>172</sup> The pledgor cannot sue because his creation of this derivative interest means that he relinquishes his right to sue third parties in conversion. Nonetheless, if there is damage to the pledgor's (reversionary) interest, he can sue for reversionary injury (for example where the damage to the pledged asset is permanent).<sup>173</sup> Thus, both the pledgor and pledgee can sue for interference – but each person has a cause of action that is underpinned by a different principle. For our purposes, we are not concerned with the 'reversionary injury' cause of action.<sup>174</sup>

The pledge is a type of derivative interest that also consists of a bailment, and can be usefully contrasted with a bailment at will, where the bailor does have title to sue for interference. Here, the bailor has title to sue because the bailor has not exercised any power to grant a derivative interest<sup>175</sup> and retains the 'right to immediate possession'. To the extent that his right to sue third parties is grounded in the notion of his 'right to immediate possession', it is suggested that this is misleading. His right to sue third parties is justified by the fact that he has title, and has not granted a derivative interest. To the extent that he has a right to immediate possession, this arises from his title,<sup>176</sup> and not the fact that under the terms of the bailment he has the right to immediate possession of the asset *as against the bailee*. He has (and often has always had) the right to immediate possession of the asset *as against the world*. In turn, the

---

<sup>171</sup> Bridge et al (n 110 above), 16-014.

<sup>172</sup> A right to immediate possession is distinct from "the right of a reversionary owner to resume possession at some future date", and in the case of the latter there is no standing to sue in conversion: Bridge et al (n 110 above), 32-035. A pledgor would fall into the latter category. Also see *Gordon* (n 164 above).

<sup>173</sup> *Obiter dicta* in *Halliday v Holgate* (1868) LR 3 Ex 299, 302; Andrew Tettenborn, 'Reversionary Damage to Chattels' (1994) 53(2) CLJ 326.

<sup>174</sup> The loss that reversionary injury is intended to protect against is not unique to situations where a derivative interest has been granted – i.e. if there is no derivative interest, the loss that otherwise would be protected by 'reversionary injury' (permanent damage etc) would still be protected. They will be protected by the other interference torts (conversion etc). For our purposes, we are focusing on the rights *lost* by the bailor, not the rights he retains (and the reversionary injury cause of action relates only to the rights that the bailor retains).

<sup>175</sup> Entering into a bailment at will is not a successful exercise of the bailor's power to grant a derivative interest to the bailee.

<sup>176</sup> In the case of a bailment where the bailor has a title to sue that arises from his 'right to immediate possession', the bailor retains his title throughout. This title confers on him a right to sue, and when he transfers possession to someone else, he relinquishes factual control, but not title.

bailee also has title to sue but this is because of his taking possession of the chattel, which gives rise to a title independent of that of the bailor.

Thus, the general position is that if a derivative interest is granted then the grantor of the derivative interest has no general right to sue for interference, and can sue only if reversionary damage occurs. In contrast, if no derivative interest is granted then there is a general right to sue for interference, not limited to cases of the sort of permanent damage that would form the basis of a claim for damage to a reversionary interest. Following this pattern, one would expect the same to be the case in relation to a chattel lease: i.e. whether a chattel lessor has the right to sue for interference would depend on whether he has granted a derivative interest.

However, as a matter of case law, it is not settled as to whether a chattel lease is a property right. Yet a chattel lessor is regarded as losing his right to sue in conversion<sup>177</sup> simply because he does not have the right to immediate possession, unlike a bailor at will.<sup>178</sup> Courts merely state that the chattel lessor does not have a right to immediate possession, or that he has ‘fragmented’ this property right without directly facing the main issue of whether the chattel lease is derivative interest, or the *numerus clausus* considerations that are relevant to this question.<sup>179</sup>

### 3.2.1.2.2 Content of a chattel lease

The case of *Gordon v Harper*<sup>180</sup> may seem to support the view that the chattel lease is a derivative interest, on the basis that the chattel lessor has fragmented his title. In *Gordon*, the

---

<sup>177</sup> (when he parts with possession of the good).

<sup>178</sup> *Bridge et al* (n 110 above), 33-036; Michael A Jones, Anthony M Dugdale, Mark Simpson, *Clerk and Lindsell on Torts* (24<sup>th</sup> edition, Sweet & Maxwell 2023), 16-61.

<sup>179</sup> See Sections 3.2.1.2.2-3.2.1.2.4 below. The *numerus clausus* principle applies to chattels: see *Bridge et al* (n 110 above), 1-060.

<sup>180</sup> *Gordon* (n 164 above).

plaintiff lessor of (*inter alia*) some furniture could not sue in conversion because he had “part[ed] with the right of possession during the term to the tenant”, and thus only had a “reversionary interest”:<sup>181</sup> only the lessee could sue in conversion. This case supports the view that the chattel lease is proprietary, for otherwise it would be extremely difficult to explain why the claimant, despite having title, loses his right to sue in conversion.

*Gordon* was cited and followed in *HSBC v Network Rail*,<sup>182</sup> albeit in the context of negligence. In *Network Rail*, it was held that the plaintiff (as a chattel lessor of train carriages) did not have the right to sue for negligence because he only had a reversionary interest. In entering into a chattel lease, he was only left with a ‘limited interest’: in other words, he had fragmented his title. The reasoning in *HSBC v Network Rail* would seem to apply to conversion too.<sup>183</sup>

In supporting the view that the chattel lease is a derivative proprietary interest, one may also point to the fact that a chattel lessee has rights against third parties. In *De Mattos v Gibson*,<sup>184</sup> Knight-Bruce LJ noted that where someone purchases or is gifted property with knowledge of a previous contract in respect of the property, “the acquirer shall not, to the material damage of the third person, in opposition to the contract and inconsistently with it, use and employ the property in a manner not allowable to the giver or seller”.<sup>185</sup> Thus, the lessee in a chattel lease can bring an action against the assignee of the ‘lessor’ if the assignee knows about the contract/lease. Knight-Bruce LJ also stated that if one acquires rights to a ship with notice of a prior charterparty, this puts him in a position of a constructive trustee, entitling the charterer to specifically enforce the charterparty against the purchaser or assignee of the vessel.

---

<sup>181</sup> *ibid*, 829.

<sup>182</sup> [2005] EWCA Civ 1437, [2006] 1 WLR 643.

<sup>183</sup> *ibid*, [29] (where Longmore LJ discusses the bailor’s limited interest in the interference tort context generally and not just in the negligence context); *Bridge et al* (n 110 above), 33-035; *The Winkfield* [1902] P 42.

<sup>184</sup> (1859) 45 ER 108.

<sup>185</sup> *ibid*, 110.

Furthermore, in *Bristol Airport v Powdrill*,<sup>186</sup> it was held (for the purpose of s.436 of the Insolvency Act 1986) that although a chattel lease is a contract, it “does not follow that no property interest is created in the chattel”.<sup>187</sup> The court noted that the chattel lease is an equitable interest, on the basis that “if under a contract, A has certain rights over property as against the legal owner, which rights are specifically enforceable in equity, A has an equitable interest in such property”.<sup>188</sup>

Indeed, the view that the chattel lease is a proprietary interest is supported by Watt,<sup>189</sup> for two main reasons. First, specific performance can be obtained against the ‘lessor’. Second, the binding effect of a chattel lease extends to third parties (as opposed to being limited to the original parties as in the case of a personal right).

However, it is suggested that a chattel lease is not in fact a derivative proprietary interest, as the rights of a ‘chattel lessee’ do not match those of a legal (or equitable) proprietary interest, but instead arise in contract with additional rights to specific performance.<sup>190</sup> As a result, it makes little sense for a ‘chattel lessor’ to lose his right to sue in conversion.

Indeed, as McFarlane<sup>191</sup> and Douglas<sup>192</sup> suggest, the chattel lease is a personal right for several reasons. First, just because specific performance is available in respect of a particular right does not mean it is proprietary.<sup>193</sup> Specific performance as a remedy is governed by whether damages provide an adequate remedy, as opposed to whether the right is capable of binding third parties.<sup>194</sup> Second, to the extent that rights are available against third parties, these

---

<sup>186</sup> [1990] Ch 744.

<sup>187</sup> *ibid*, 759.

<sup>188</sup> *ibid*, 759.

<sup>189</sup> Graeme Watt, ‘The proprietary effect of a chattel lease’ (2003) Conv 61.

<sup>190</sup> Ben McFarlane, ‘Identifying property rights: a reply to Mr Watt’ [2003] Conv 473.

<sup>191</sup> *ibid*.

<sup>192</sup> Douglas (n 2 above), chapter 3.

<sup>193</sup> See e.g. *National Provincial Bank v Ainsworth* [1965] AC 1175 at 1253 (Lord Wilberforce): “The fact that a contractual right can be specifically performed, or its breach prevented by injunction, does not mean that the right is any the less of a personal character or that a purchaser with notice is bound by it: what is relevant is the nature of the right, not the remedy which exists for its enforcement”.

<sup>194</sup> *ibid*, 35.

rights may be new rights as opposed to the continuation of an old right.<sup>195</sup> Third, the remarks in *De Mattos* can be interpreted as referring to the doctrine of inducing breach of contract, where a defendant is liable to a claimant when he takes action to procure a breach of contract in a situation where he knows about the contract between the claimant and a third party (i.e. the lessee and the lessor), realises that there would be a breach and intends to procure such a breach.<sup>196</sup> The ability to sue someone for inducing breach of contract does not mean that the contractual right is proprietary.

The notion that chattel leases are proprietary interests has also been criticised on other grounds. If the interest of a chattel lessee is an equitable interest under a trust, it is unclear what the subject-matter of the trust is.<sup>197</sup> It cannot be title to the chattel itself, otherwise the chattel lessee can demand a conveyance of (legal) title to the goods under *Saunders v Vautier*. It also cannot be the lessee's rights under the contract: for such rights to be held on trust *for* the lessee, they must be held by someone other than the lessee. The lessor has contractual obligations to the lessee but obligations cannot be held on trust.<sup>198</sup>

Thus, if the chattel lease is not a derivative proprietary interest, the chattel lessor ought not to lose the right to sue in conversion. The current position is therefore wrong in principle, and should not be replicated in the digital asset context.

### 3.2.1.2.3 Language of 'right to immediate possession'

---

<sup>195</sup> McFarlane (n 191 above), 477-480.

<sup>196</sup> *Lumley v Gye* (1853) 2 E&B 216; *OBG* (n 123 above), [39] and [62].

<sup>197</sup> William Swadling, 'The Proprietary Effect of a Hire of Goods' in Norman Palmer and Ewan McKendrick, *Interests in Goods* (2<sup>nd</sup> ed, London 1998), 499-500; Susan Bright, 'The Third Party's Conscience in Land Law' [2000] Conv 398.

<sup>198</sup> Swadling (n 197 above), 499-500; *Port Line Ltd v Ben Line Steamers Ltd* [1958] 2 QB 146, 163, 166-167.

This confusion<sup>199</sup> is inextricably linked to the fact that the language of ‘right to immediate possession’ is inherently vague and does not provide much guidance. It is unhelpful insofar as ‘right to immediate possession’ is synonymous with ‘right to sue for interference with possession’. It is also unhelpful insofar as a person with title to the goods already has the right to possess the goods. It is difficult to know what ‘immediate’ means, and this creates confusion.<sup>200</sup>

This label allows judges to duck the question of whether the chattel lease is fully proprietary.<sup>201</sup> It also allows judges to duck the underlying *numerus clausus* question of whether the reasons in favour of recognising a new proprietary interest in goods (the chattel lease) outweigh the reasons against. In so doing, it importantly allows judges to duck the overarching normative debate around when exactly a person should have title to sue for interference.

If we import this ‘right to immediate possession’ doctrine into the digital asset space, all these questions can be ducked *in the digital asset context too*. The doctrine can once again become a fig-leaf, and a conclusion can masquerade as reasoning, bootstrapped by technical language that gives it the appearance of legitimacy. As a result, the court’s reasoning would become very opaque, and judges would be given a chance to avoid these very important questions that need to be answered to provide clarity as to people’s rights.

As a result, arbitrary decisions can be reached, the court’s reasoning will be less rigorous, and bad analogies can be drawn because the rule does not give much guidance.<sup>202</sup> We see this in other contexts too, for example in administrative law. The labels of ‘illegality’, ‘error

---

<sup>199</sup> I.e. the conceptual confusion in relation to chattel lessors losing the right to sue in conversion despite the chattel lease not being a proprietary interest.

<sup>200</sup> This confusion may be one of the reasons why there has been some dicta to the effect that a *contractual* right to possession may suffice for a claim in conversion, without any proprietary rights: see nn 212-213 below and text thereto.

<sup>201</sup> In the sense of conferring non-interference rights effective against the world.

<sup>202</sup> See Section 3.2.2.1 below.

of law’ and ‘error of fact’ allow a court to come to a normatively desirable conclusion first and use these labels as grounds for its conclusion, even if there is no satisfactory reasoning.<sup>203</sup>

#### 3.2.1.2.4 Starting afresh, and the numerus clausus

Given the confusion regarding the nature and content of the rights of a chattel lessee, it is suggested that this jurisprudence should not be followed and/or applied in the digital asset context. We should instead directly analyse the ‘title to sue’ issue from the perspective of whether a derivative legal property right should be recognised in situations such as (for example) the ‘digital equivalent’ of a chattel lease.<sup>204</sup> This necessitates a systematic approach whereby we analyse the reasons for (and against) the recognition of a proprietary interest, and (if we allow such an interest) make sure its content conforms with the content of a proprietary right.

This question should be determined in accordance with numerus clausus considerations. As McFarlane notes, the recognition of a new property interest under the numerus clausus can only take place after the benefits of doing so are balanced against the harms of doing so (and determining that the former outweigh the latter).<sup>205</sup> Most notably, as recognising a new property interest necessarily involves a constraint on the liberty of third parties, this concern must be taken into prime consideration when deciding whether to allow parties the freedom to create a new interest.<sup>206</sup> Other policy considerations that ought to be taken into account include

---

<sup>203</sup> Elliott and Varuhas make this point when discussing the judgments of Lord Hope and Lord Carnwath in *Jones v First-Tier Tribunal* [2013] UKSC 19, [2013] 2 AC 48. See Mark Elliott and Jason Varuhas, *Administrative Law: Text and Materials* (5<sup>th</sup> ed, OUP 2017) 64: “On this approach, ‘law’ and ‘fact’ serve as little more than conclusory labels signalling that, for other reasons, a particular degree of judicial intervention has been judged to be normatively warranted.” This finds support from [46] of the judgment (Lord Carnwath). See also *R (Privacy International) v Investigatory Powers Tribunal* [2019] UKSC 22, [2020] 2 AC 491, [79]-[84].

<sup>204</sup> I.e. a contractual right to exclusive control of a digital asset for an agreed period.

<sup>205</sup> Ben McFarlane, ‘The Numerus Clausus Principle and Covenants Relating to Land’ in Susan Bright (ed), *Modern Studies in Property Law* (Volume 6, Hart Publishing, 2011) 311, 317-318.

<sup>206</sup> *ibid*, 318.

(e.g.) information costs and adjudication costs,<sup>207</sup> and the potential consequences to both (a) transferees/successors in title, and (b) trespassers/those who have interfered in some way with the property.<sup>208</sup>

There is not much case law on digital assets, meaning that the law can start from a clean slate in the sense that it does not need to be constrained by the current law on chattel leases and possession. A new digital assets regime can be formulated, such that the ‘digital lease’ issue can be examined afresh, and the underlying principles and doctrines in the physical asset (and possession) context can be seen as general reference points that can be applied or deviated from.<sup>209</sup>

This leaves open the possibility that an arrangement in the digital asset context that is similar to a term bailment would constitute a ‘digital lease’. This could contain rights and remedies available to the ‘lessor’ (that correspond with ‘reversionary damage’) and the ‘lessee’ (that correspond with ‘trespass’ or ‘conversion’).

Ultimately, whether such a development will occur depends on the costs and benefits mentioned above<sup>210</sup> as applied to the digital asset context. Space precludes a detailed examination of these costs and benefits, but the first step towards doing so is to identify the debate (and the relevant considerations) to which the issue relates.

### ***3.2.2 Differences between physical and digital assets***

Even if it is assumed that the possession-dependent rules are satisfactory in the physical asset context, extending these rules to digital assets would be undesirable. This is because possession

---

<sup>207</sup> *ibid*, 318.

<sup>208</sup> *ibid*, 315.

<sup>209</sup> Analogies and distinctions can be made at the ‘substance’ and ‘technique’ levels.

<sup>210</sup> See McFarlane (n 205 above), 320 and text to nn 204-209 above.

is a doctrine designed for physical assets, and there are many differences between physical and digital assets, making possession a bad fit in the digital asset context.

For example, while physical assets can exist out in the open and can move through continuous spaces relatively freely, digital assets can only exist in particular locations (public addresses) and their movement resembles ‘jumping’ from location to location as opposed to moving continuously through space. Also, while movable physical assets can take a long time to be transported from place to place, digital assets can be transferred to public addresses nearly instantaneously. Furthermore, humans can interact with physical assets by interacting with the physical environment (without the aid of anything digital) and can ‘break in’ to particular spaces by brute force. In contrast, with digital assets, one needs to interact with a computer system and generally cannot ‘break in’ to particular spaces or smart contracts except by interacting with the code or executing functions on a computer (which would usually require knowledge of someone’s private key). All these differences stem from the fact that physical assets obey the laws of physical reality (gravity etc), while digital assets depend on computer code (and are ideational because people can conceive of the ‘digital environment’ in different ways when attempting to ‘translate’ digital language into understandable analogies/comparisons).

What are the effects of applying possession to digital assets despite such differences? First, policies and features in the physical asset world may mistakenly be seen as relevant in deciding a digital asset case, as cases in the digital asset context that engage with the possession issues will inevitably draw upon analogies from the physical asset context. Second, the reverse may also happen: policies and features in the digital asset world that are fundamentally irrelevant may be mistakenly seen as relevant or decisive in the context of deciding a particular case. These mistakes can be easy to make especially as (1) the blockchain space is relatively

new and shrouded in technical jargon, and (2) the existing rules on possession are archaic and can date back to the 18<sup>th</sup> century.

### 3.2.2.1 Errors in applying the ‘right to immediate possession’ concept

The fact that physical and digital assets are vastly different in nature means that when combined with messy legal rules, decisions in the digital asset world may be very random. For example, applying the ‘right to immediate possession’ in the digital asset context can lead judges into making errors and/or unpredictable decisions. Suppose that X owns a crypto-token that (by way of smart contract) allows him to redeem an underlying cryptocurrency (let us say Ether) on demand from a counterparty (for example under a wrapping protocol),<sup>211</sup> under which the Ether is deposited in the counterparty’s wallet. If the wallet that contains the underlying Ether is hacked by a thief, and the counterparty no longer has the funds to sue (or actively refuses to sue), X may want to sue the thief directly for tortious interference. If possession (and conversion) were to apply to digital assets, a judge would need to consider whether X has possession or a ‘right to immediate possession’. X does not have possession of the underlying Ether as it is deposited in the counterparty’s wallet, but the issue would be whether X’s ownership of the token, which allows him to redeem (and thus take control of) the Ether on demand (as specified by the conditions of the smart contract), means he has a ‘right to immediate possession’ of the underlying Ether.

A judge may be sympathetic with X and may thus point to the automated nature of smart contracts in supporting the conclusion that there is a right to immediate possession. The right to obtain possession is ‘immediate’, much more so than for physical assets where there

---

<sup>211</sup> A wrapping protocol converts a token from one blockchain (X) into a token on another blockchain (Y) that represents the original token X.

are usually much longer time delays before an asset is obtained (for example in the shipping context where the holder of a bill of lading can have a ‘right to immediate possession’ but the goods may not be in the possession of the holder until months later). This would be supported by the fact that the ‘immediate’ right to obtain the Ether is stated in the contract with X’s counterparty, and a judge may rely on dicta in (for example) *Iran v Barakat*<sup>212</sup> as well as *Simgood Pte Ltd*<sup>213</sup> to the effect that a contractual right to possession can constitute a ‘right to immediate possession’.

However, this would result in a poor conclusion reached through poor reasoning. In this case, X has no proprietary right to the Ether tokens themselves, meaning that there is no right to immediate possession.<sup>214</sup> Reaching the opposite conclusion is unsatisfactory for three reasons.

First, having a mere contractual right to possession does not suffice to bring a claim against a third party as demonstrated by *Jarvis v Williams*.<sup>215</sup> The prevailing view is that a legal proprietary right is a necessary condition for a ‘right to immediate possession’ to exist.<sup>216</sup>

Second, the reasoning based on ‘immediacy of execution of smart contracts’ relies on a feature of digital assets<sup>217</sup> that is irrelevant to the normative threshold. What matters for the requirement is the nature of the legal right, not the technical features/specifications of a smart contract (unless they affect the nature of the right itself).

Third, allowing a person with a mere contractual right to possession to sue for conversion would effectively impose strict liability for certain interferences with contracts,

---

<sup>212</sup> *Government of the Islamic Republic of Iran v Barakat Galleries Ltd* [2007] EWCA Civ 1374, [2009] QB 22, at [26] and [30].

<sup>213</sup> *Simgood Pte Ltd v MLC Shipbuilding Sdn Bhd* [2015] SGHC 303, [153] and [154].

<sup>214</sup> *Jarvis v Williams* [1955] 1 WLR 71.

<sup>215</sup> *ibid.* Also see e.g. *Bridge et al* (n 110 above), 33-039; *Jones et al* (n 178 above), 16-62; Nicholas Curwen, ‘Title to sue in conversion’ (2004) Conv 308. Equitable rights are not sufficient either: see *MCC Proceeds v Lehman Brothers International (Europe)* [1997] EWCA Civ 3068, [1998] 4 All ER 676.

<sup>216</sup> See e.g. *Bridge et al* (n 110 above), 33-039; *Jones et al* (n 178 above), 16-62; Curwen (n 215 above), 309, 314-316.

<sup>217</sup> I.e. automatic and quick execution.

which would go against the general approach in *Lumley v Gye*.<sup>218</sup> The economic tort of inducing breach of contract governs the scope of when it is legitimate to interfere with a contract. As clarified in *OBG*, the mental element of the tort requires the defendant to know of the contract and realise that the relevant conduct would amount to a breach of contract, as well as to intend to induce the breach of contract.<sup>219</sup> This is a fault standard, as opposed to a strict liability standard. Furthermore, even though Lord Nicholls and Lady Hale in *OBG* were in favour of extending conversion (a strict liability tort) to purely contractual rights, this suggestion was rejected by the majority.<sup>220</sup> Thus, the principle that there cannot be strict liability for interferences with contracts is well-entrenched in English law.

No doubt a finding for X in the example might be motivated by the fact that a contractual right to possession plus immediacy of execution produces a similar factual position to having actual possession or the immediate ability to obtain possession under a property right. However, the importance of ensuring that the similarities in question are *relevant* cannot be overstated. For example, in *Shell UK Ltd v Total UK Ltd*,<sup>221</sup> the Court of Appeal held that a beneficiary under a trust had sufficient title to sue a third party for negligence, by drawing an analogy with the position of a legal owner.<sup>222</sup> This decision has been widely criticised (and rightly so):<sup>223</sup> the right to sue for negligence is premised on having a right to possession, and a beneficiary qua beneficiary simply does not have the right to possession. Similarly, in the conversion context, one must not conflate a right to possession of the asset against a particular counterparty (contract) and the right to possession of an asset generally against the world (property): it is only the latter that suffices for the purposes of title to sue.

---

<sup>218</sup> *Lumley v Gye* [1853] EWHC QB J73; Curwen (n 215 above), 316-317.

<sup>219</sup> *OBG* (n 123 above), [39] and [62].

<sup>220</sup> See section 3.1.1 above.

<sup>221</sup> [2010] EWCA Civ 180, [2011] QB 86.

<sup>222</sup> See e.g. *ibid*, [142]-[144].

<sup>223</sup> See e.g. James Edelman, 'Two fundamental questions for the law of trusts' (2013) 129 LQR 66, 69-72; PG Turner, 'Consequential economic loss and the trust beneficiary' (2010) 69 CLJ 445; Emma Hargreaves, 'The nature of beneficiaries' rights under trusts' (2011) 25 TLI 163, 165-166.

Yet, it is easy to make such mistakes because the technology is new, and the language of ‘immediate’ possession is apt to mislead.<sup>224</sup> Applying the same phrase to a new area/asset introduces uncertainty in interpretation, and leaves the door open for new arguments based on the nature of the new asset. A judge might be persuaded by an argument that the position concerning digital assets should be claimant-friendly in terms of granting title to sue, and correspondingly adopt (e.g.) a wider interpretation of ‘immediate’ and thereby conflate fact and right. Given the ‘code is law’ school of thought, it may be easy to conflate fact and right.<sup>225</sup>

### 3.2.2.2 Effects on the physical asset threshold

Extending possession to digital assets can carry further knock-on effects on the *physical* asset threshold, because it reduces the necessary conditions for the concept of possession to apply. Traditionally, possession requires a person to touch the molecules of an object or be in close proximity to the object,<sup>226</sup> but if possession were to apply to digital assets, there would no longer be a ‘close proximity’ requirement.

This is because (e.g.) if someone transfers a bitcoin into my address, I do not have to be in close proximity to any molecules. Since Bitcoin is an ideational asset, it is not made up of any molecules.<sup>227</sup> This is the case even though the molecules that constitute the underlying computer infrastructure etc are *required* for Bitcoin to exist: these molecules do not form *part* of the Bitcoin. To have positive and negative control of a Bitcoin in my address, I do not even need to be in close proximity to any molecules that are necessary for the Bitcoin to exist, as,

---

<sup>224</sup> One may, quite naturally, interpret ‘immediate’ as denoting factual immediacy instead of a particular type of legal property right, especially in the blockchain context where the technology is new and there is relatively little certainty as to people’s legal rights.

<sup>225</sup> ‘Code is law’ is a school of thought to the effect that people’s legal rights are governed by the code itself: see e.g. Lawrence Lessig, *Code: And Other Laws of Cyberspace, Version 2.0* (Basic Books, 2006), 5, 77.

<sup>226</sup> See e.g. *Borwick Development v Clear Water Fisheries* [2020] EWCA Civ 578, [2021] Ch 153.

<sup>227</sup> See e.g. Craig Warmke, ‘What is Bitcoin’ (2021) Inquiry 1.

for example, miners with full nodes can be halfway across the world. Thus I do not need to be in close proximity to any molecules to take ‘possession’ of Bitcoin.

This argument could then be relied upon in the physical asset context. Suppose an AI/self-driving/computer-programmed car company (Y) lets one of its cars out to X on hire purchase or under some kind of lease arrangement. Under this arrangement, Y retains control over the car and can direct the movement of the car, but X can also do so through (for example) moving the steering wheel. The car is damaged by D, and Y wants to sue the defendant for conversion. Here, Y does not have a ‘right to immediate possession’ since this arrangement involves a hire purchase/term bailment. Nonetheless, it may argue that it has ‘possession’ of the car. Since there would be no ‘close proximity’ requirement for possession, and since Y retains control over the car, it is irrelevant that Y controls the car from (e.g.) the head office miles away from the actual car. This may constitute ‘possession’, and the claim would on this basis be granted.

Granting the claim would thus disrupt the threshold for physical assets, as it dispenses with the ‘close proximity’ requirement for possession of regular physical assets (such as cars). The root cause of this is ‘over-lumping’,<sup>228</sup> i.e. extending a concept beyond what it is designed for. Making such an extension reduces the threshold required for the concept to apply, and allows this reduced threshold to ‘contaminate’ or ‘disrupt’ other areas where the same concept (possession) applies. Even if the conversion argument ultimately does not succeed before a court, this does not detract from the fact that the ‘over-lumping’ creates the (serious) possibility of these types of arguments being made, and thus introduces uncertainty in relation to the existing rules for physical assets. Indeed, as the Law Commission note, it is not preferable to

---

<sup>228</sup> This term is used in one of my articles: Hin Liu, ‘Title, control and possession in the digital asset world’ [2022] LMCLQ 597, 615.

“stretch...the concept of possession to the point where it snaps or modify...it to the point of disfigurement”<sup>229</sup> by applying it to digital assets.

### 3.2.3 An ‘on-off’ switch?

Nonetheless, one may object to the above analysis and argue that it is possible to use ‘possession’ to govern the question of acquiring an original title to digital assets, without necessarily having the other possession-dependent doctrines apply to such assets.

There are two responses. First, even if a court ends up concluding that a particular possession-dependent doctrine should not apply to digital assets, the possession argument would need to be considered. In other words, since people attach consequences to the characterisation of a digital asset as ‘possessable’, one has to specifically explain why a normal consequence of possession should *not* apply to digital assets, as opposed to why it should. In this sense, there is a certain ‘path-dependence’ if the law decides that digital assets are possessable. The normative default would be that possession-dependent doctrines apply, so courts may be naturally more resistant to arguments that seek to disapply certain possession-dependent doctrines (compared to if possession were not to apply to digital assets).

Thus, even if a particular doctrine or concept is unsatisfactory (e.g. bailment or a ‘right to immediate possession’), it may take much longer for a court to be persuaded by a convincing argument in favour of disapplying any possession-dependent consequence or doctrine since the court needs to be persuaded to *depart* from an established concept and cause potential ‘incoherence’ or ‘inconsistency’ in the law. In contrast, if possession is limited to physical assets, there would be no issues of path-dependence or ‘incoherence’. Each consequence that would result from applying possession-dependent doctrines can be considered in the digital

---

<sup>229</sup> Law Commission, *Consultation paper* (n 8 above), 11.69.

asset context in a way that is free of the shackles of possession jurisprudence, which would enable the court's reasoning to be transparent, with the normative balance considered afresh.

Nonetheless, physical asset analogies would still remain highly relevant to the court as they may draw on such analogies as part of their reasoning. Thus, the court (or legislature) would not be starting wholly from scratch. In this context, the main advantage is that the court (or legislature) has the flexibility to deviate from the position in relation to physical assets if it is thought to be unsatisfactory, yet can draw on relevant physical asset analogies as part of their reasoning process. Analogies can be drawn at the 'aim', 'substance', or 'technique' levels, and distinctions can be drawn at the 'substance' and 'technique' levels.

#### ***3.2.4 Practical effects in the litigation context***

Applying possession to digital assets would also create deleterious consequences in the litigation context. First, counsel can raise extensive 'possession-based' arguments on both sides that have some 'doctrinal possibility' of succeeding, even if they are arguments that have no merit from a normative standpoint. Second, judges would as a result have to go through much more material. Even if they end up rejecting a possession argument, they may have to spend a lot of unnecessary time justifying why the argument fails.<sup>230</sup> Third, interlocutory applications (such as summary judgment and strikeout applications) might fail on the basis that there is a 'triable issue' or '*prima facie* case' based on possession, even when from a normative standpoint they should straightforwardly succeed. These three factors lead to a severely inefficient use of limited court resources, as time and cost are wasted on irrelevant and/or tangential issues.

---

<sup>230</sup> This happens with courts in general: see e.g. Henry Litton, *Is the Hong Kong Judiciary Sleepwalking to 2047?* (Sherriff Books, 2019) 119.

### 3.3 Control

Instead of possession, it is suggested that the concept of ‘control’ should be used, as it reflects the normative threshold set out in Section 2 and avoids the disadvantages previously mentioned in relation to ‘possession’. ‘Control’ is also consistent with the rationales examined in Section 2.2 for allowing property rights to be acquired through possession. Using a threshold of ‘factual positive and negative control’ avoids many of the problems with ‘possession’ but fulfils the same normative job. Furthermore, the use of concepts other than ‘possession’ or ‘control’ create unacceptable uncertainty and complexity.

In reaching this conclusion, I will explore (1) the concept and meanings of control, (2) the advantages of using control over possession, and (3) why we should not use any other concept.

#### 3.3.1 *The concept and meanings of control*

In many contexts, possession and control are used interchangeably.<sup>231</sup> There are indeed many similarities between the two concepts, as both encompass the idea that one is able to put an object or asset to its uses (positive control), and/or prevent others from being able to put the object or asset to its uses (negative control).<sup>232</sup> Also, both concepts can be understood in the factual sense (one’s practical ability to put the object to its uses and/or prevent others from

---

<sup>231</sup> For example in the Financial Collateral Arrangements (No 2) Regulations 2003 (SI 2003/3226) (“FCARs”): see FCAR Reg 3.

<sup>232</sup> See also Law Commission, *Consultation paper* (n 8 above), 11.91 (‘control’ of a digital asset as encompassing a sufficient degree of positive and negative control).

doing so) or in the legal sense (the right to obtain the practical ability to use an asset,<sup>233</sup> and/or the right to prevent another person from being able to make use of an asset<sup>234</sup>).

Nonetheless, ‘control’ is a much broader concept. If one attempts to find the paradigm case of ‘control’, he could say that a (healthy) person has an extremely high level of control over his hands and arms, as he is able to influence the movement of his arms, and he is able to stop others from moving them (and is thus able to put his hands and arms to their uses and prevent others from doing so). We would also say that, by extension, holding a physical object (such as a smartphone) with one’s hands indicates a high degree of control over the smartphone.

However, this is just one possible paradigm, and one might equally say that the paradigm case of ‘control’ refers to the ability to dictate behaviour, such as in the case where a boss or parent is being ‘controlling’. This is a far cry from exerting *physical* control over a object (or even a person), yet it is strongly arguable that the second notion of control is the paradigm case.

Indeed, these two meanings are seen in different legal contexts. In classifying whether a person is an employee or an independent contractor, the touchstone had for a long time been ‘control’.<sup>235</sup> The factors used in determining whether such control exists include whether the ‘employer’ is able to supervise and dictate the “manner in which the work [is] done”<sup>236</sup> (instead of the employee being granted a high degree of freedom). If the threshold of ‘control’ is satisfied, the worker would be considered an ‘employee’. This carries various legal consequences such as the worker being entitled to statutory benefits,<sup>237</sup> as well as tort victims being able to sue the employer for vicarious liability.<sup>238</sup> It is clear that in this context, ‘control’

---

<sup>233</sup> Legal positive control, e.g. constructive possession in the bills of lading context (see nn 110-112 above and text thereto).

<sup>234</sup> Legal negative control, e.g. in the FCARs context: see n 244 below and text thereto.

<sup>235</sup> Jones *et al* (n 178 above), 6-04 (and cases cited therein).

<sup>236</sup> *ibid*, 6-04.

<sup>237</sup> See e.g. Employment Rights Act 1996, National Minimum Wage Act 1998, Employment Relations Act 1999, Equality Act 2010.

<sup>238</sup> Jones *et al* (n 178 above), 6-04; but note recent vicarious liability cases where control in this sense is not seen as necessary. See, e.g. *Barclays Bank v Various Claimants* [2020] UKSC 13, [2020] AC 973, [20].

is used in the sense of ‘influence over one’s behaviour’. In contrast, having factual possession of a physical asset is often described as ‘exclusive physical control’,<sup>239</sup> and this clearly refers to the first meaning of being able to put an object or asset to its uses and prevent others from being able to do so, and in the factual sense.

Also, in the security interest context, the use of ‘control’ clearly refers to the first meaning. A charge is characterised as fixed as opposed to floating if the chargee exerts a sufficient degree of ‘control’ over the charged asset, and what is required in (for example) the book debts context is essentially that the debts have to be deposited into an account from which the chargor is not allowed to withdraw.<sup>240</sup> In this situation, the chargee has ‘control’ over the book debts because he is able to prevent the chargor from moving the book debts out of the account.<sup>241</sup> A similar approach is adopted in the Financial Collateral Arrangements (No. 2) Regulations 2003 (“FCARs”),<sup>242</sup> where special consequences follow if the asset that is the subject of the security is in the ‘possession or control’ of the security-taker.<sup>243</sup> In this context, ‘control’ is interpreted as meaning negative legal control of the asset in question<sup>244</sup> (the right to prevent another person from making use of the asset).

In the digital asset context, it is clear that one would not be using ‘control’ in the sense of being able to influence someone’s behaviour (as a digital asset is not a person). We would clearly be using ‘control’ in the sense of the ability to put an object or asset to its uses and prevent others from doing so.

---

<sup>239</sup> *Powell v McFarlane* (n 17 above), 470-471; *Pye* (n 103 above), [41]; *Rostill* (n 13 above), 15-19.

<sup>240</sup> *Re Spectrum Plus* [2005] UKHL 41, [2005] 2 AC 880, especially at [55].

<sup>241</sup> Note that the account must as a matter of *substance* be operated as a blocked account: see Roy Goode and Louise Gullifer, *Goode and Gullifer on Legal Problems of Credit and Security* (6<sup>th</sup> ed, Sweet & Maxwell 2017), 4-22; *Agnew v Commissioners of Inland Revenue* [2001] UKPC 28, [48].

<sup>242</sup> SI 2003/3226 (see n 231 above).

<sup>243</sup> It would qualify as a ‘security financial collateral arrangement’ under FCAR Reg 3, which has various consequences regarding (e.g.) the disapplication of formalities and on insolvency: see FCAR Parts 2, 3 and 4.

<sup>244</sup> *Gray v G-T-P Group Ltd* [2010] EWHC 1772 (Ch), *Re Lehman Brothers International (Europe) (In Administration)* [2012] EWHC 2997 (Ch); *Private Equity Insurance Group SIA v Swedbank AS (C-156/15)* [2017] EU:C:2016:851; 1 WLR 1602; [2017] 1 BCLC 207 though note that this threshold is controversial among academics: see e.g. Goode and Gullifer (n 241 above), 6-44.

We would also be using it in a factual sense instead of a legal sense, since obtaining control of a digital asset in the manner mentioned in Section 2.2 does not require the tokenholder to enter into any legal agreement.

### ***3.3.2 Advantage of using control over possession***

The main advantage of using control is it does not have physical connotations, and so the concept need not be distorted when applying it to digital assets. The concept of control already covers all kinds of property, tangible and intangible, in contrast with possession (which only covers a subset of property (tangible property)). Unlike ‘possession’, there is no need to distort ‘control’ to cover a new situation it is not designed to cover. This avoids bad outcomes associated with such distortions: e.g. there is no need to be swayed by bad/irrelevant analogies in the physical asset context.

Fundamentally, the significance of ‘control’ being a concept that does not have physical connotations (unlike possession) is that there is nothing unnatural about extending the concept to digital assets. Indeed, the concept of ‘control’ has two clear meanings, and as long as we know which meaning is being used, ‘control’ generates much better results (and is a much better tool for judges) than ‘possession’. If we adopt ‘possession’, there is a need to reconcile the inherent physicality of the concept (as demonstrated by, e.g. *OBG*)<sup>245</sup> with its extension to the digital asset world. There would be a need to make sure that the concept of digital possession is ‘close enough’ to the concept of physical possession in order to prevent any knock-on effects on the physical asset threshold. Yet, this may not produce the correct threshold for digital assets.

---

<sup>245</sup> See discussion of *OBG* (n 123 above), at section 3.1.1 above.

In addition, judges do not speak with one voice in relation to what is considered necessary and sufficient for the ‘possession’ concept (or sub-concepts of possession) to come into play. Yet, although applying possession to new contexts reduces these necessary conditions (i.e. applying possession to digital assets renders it unnecessary for there to be close proximity with molecules that form an object), this ‘reduction’ in necessary conditions is only appropriate for one *sub*-concept (possession as applied to *digital* assets). It is inappropriate for possession as applied to physical assets (another sub-concept).

If judges are unaware of these changes, the fact that the same concept or word applies to both types of assets means that there is a natural tendency to assume that the new (relaxed) threshold applies across the board. The fact that possession is already used and applied in such a confusing and ambiguous way means that the (appropriate) distinctions between the two types of assets may well be conflated, and wrong analogies may be drawn. This creates further knock-on effects on the physical asset threshold), because the differences are inappropriately obscured.<sup>246</sup>

There is no such problem with ‘control’, since applying control to digital assets does not involve a ‘shift’ or ‘reduction’ in the necessary conditions required for the concept to apply. As Moore-Bick LJ noted in *Your Response*, (practical) control is a wider concept than possession, and it can extend to the intangibles context.<sup>247</sup> Thus, applying ‘control’ to digital assets would not distort its meaning – this stands in stark contrast to ‘possession’.<sup>248</sup>

Indeed, the common feature between ‘digital possession’ and physical factual possession is control. An asset is subject to a person’s (exclusive) control – if it is a physical asset, physical control is required; if it is a digital asset, digital control is required. Thus, it

---

<sup>246</sup> See Section 3.2.2.2 above.

<sup>247</sup> *Your Response* (n 122 above), [24].

<sup>248</sup> In addition, the Law Commission has noted that the law of England and Wales is “familiar with applying notions of control to both tangible and intangible objects of personal property rights”: see Law Commission, *Consultation paper* (n 8 above), 11.79.

would be preferable to directly use the concept of control instead of using possession.<sup>249</sup> As ‘control’ represents the ‘common ingredient’, it also does the same normative work that is done by ‘possession’.<sup>250</sup> Using ‘possession’ obscures the element that is important, i.e. control, not physicality. This increases the time required for judges to be clear on the necessary threshold, and may cause judges to misunderstand the threshold and/or draw incorrect analogies, thereby reaching incorrect decisions. This increases information and adjudication costs, which would be saved if ‘control’ is adopted. By adopting ‘control’, the negative consequences of distorting a concept too far past its natural or paradigm case would be averted.

Also, with ‘control’, there is no ‘on switch’ issue relating to possession-dependent doctrines, since we would not be presumptively forced to adopt possession-based doctrines. If the court wishes to depart from an outcome that would otherwise result from applying possession to digital assets, there is no need to waste time on arguments on why certain possession-dependent doctrines should not be applicable. We can deal with questions such as acquisition of title and interference without being constrained by possession jurisprudence.

Fundamentally, people do not attach specific consequences to an item of property that is ‘controllable’: they only assume the regular consequences of something being property, because control (or exclusive control) is one of the general requirements for title to arise in the first place.<sup>251</sup> In contrast, as only certain items of property can be ‘possessed’ (and specific legal consequences apply to such items of property), people would attach these consequences (e.g. bailment, conversion etc) to a new class of property if possession is considered applicable to it. Removing this uncertainty and confusion allows the normative debate to take place in an open and transparent manner.

---

<sup>249</sup> (In the digital asset context)

<sup>250</sup> I.e. it performs the functions discussed in Section 2.2.

<sup>251</sup> See e.g. Bridge *et al* (n 110 above), 1-006.

Confining ‘possession’ to physical assets also avoids the replication of bad rules in the digital assets, but it could be argued that ‘control’ is also confusing and gives rise to many problems. For example, there are various uncertainties as to the threshold of ‘control’ required for a fixed charge,<sup>252</sup> as well as the notion of ‘possession or control’ for the purpose of the FCARs.<sup>253</sup>

In the FCARs context, it is controversial as to whether if the collateral-taker has legal control but not factual control, that would be sufficient to satisfy the threshold of ‘possession or control’ as required by the FCARs to perfect the relevant security interest. An example of such a situation would involve a collateral-taker who enters into a (legal) agreement with the collateral-provider whereby the latter is obliged not to withdraw from the account in which the charged assets are located, but can (factually) withdraw money from the account (despite this being a breach of contract). On the one hand, Goode and Gullifer note that if there is no factual control, this would not fulfil the ‘publicity function’ and thus go against the policy of the FCARs in introducing this provision, which is to prevent fraud. As such, “it might seem that both legal and [factual] control are required for a security arrangement to fall within the FCARs”.<sup>254</sup> On the other hand, Briggs J in *Re Lehman Brothers International (Europe)*<sup>255</sup> raised a situation where the collateral is in the possession of the collateral-provider but the collateral-taker has the right to ensure that the collateral is used in accordance with its directions, which would be (in Goode and Gullifer’s words) “presumably sufficient to fall within the FCARs”.<sup>256</sup> Thus, one may object to the use of the ‘control’ concept on the basis that it too causes much confusion and controversy.

---

<sup>252</sup> See e.g. Louise Gullifer, ‘The Reforms of the Enterprise Act 2002 and the Floating Charge as a Security Device’ (2008) 46 Can Bus LJ 399, 424-427.

<sup>253</sup> Goode and Gullifer (n 241 above), 6-44.

<sup>254</sup> *Ibid*, 6-44.

<sup>255</sup> *Lehman* (n 244 above), [136].

<sup>256</sup> Goode and Gullifer (n 241 above), 6-44.

However, this objection is misdirected. The confusion about ‘control’ in the FCARs/charges context is not because the concept of ‘control’ is vague, but rather because the normative/policy balance that ought to be struck in those particular contexts requires a very specific type and degree of control that must comport with the statutory purpose of the FCARs. This is especially so given the EU backdrop to the debate.<sup>257</sup> In other words, there is a mismatch between the threshold in the case law (legal control being necessary) and the standard normatively demanded by the FCARs/FCD<sup>258</sup> (which Goode and Gullifer argue ought to be factual control).

In fact, if ‘possession’ (instead of ‘possession or control’) were the test in the FCARs context, the law would be rendered even *less* coherent since (1) possession would need to be stretched to apply to intangibles (the pitfalls of which have already been explored), and (2) applying possession to a context that requires such a delicate policy balance is liable to distort the law even more, and lead to judges applying the law incorrectly and/or drawing the wrong analogies. Control is, therefore, already the better concept to apply in the FCARs context.

In the digital asset context, we do not need to concern ourselves with the specific policy balance of the FCARs (and the debate as to what this policy balance demands as a legal requirement). The confusions and problems associated with this are avoidable as long as we are clear enough on the meaning of ‘control’ for our purposes. Here, we are referring to the existence of positive factual control (the ability to transfer the asset on-chain), and negative factual control (the ability to use one’s private key to exclude others). There are uncertainties at the borderline as to (for example) the number of confirmations required for title to be acquired,<sup>259</sup> but the threshold of ‘control’ for the purposes of digital assets is relatively

---

<sup>257</sup> See, e.g. *ibid*, 6-43 and 6-44. There may be a mismatch between the legal threshold envisaged by Briggs J in *Lehman* (n 244 above) and the policy of the FCARs.

<sup>258</sup> The FCARs implement the FCD (Financial Collateral Directive) ie Directive 2002/47/EC of the European Parliament and of the Council of 6 June 2002 on financial collateral arrangements.

<sup>259</sup> See text to nn 25-26 above.

determinate, and arguably even more so than in relation to certain types of physical assets.<sup>260</sup> For example, it is difficult to say where the dividing line is in terms of when one ‘controls’ a big ship that is physically difficult to handle.

Overall, this meaning of ‘control’ can be clearly distinguished from (1) legal control (a legal right to prevent another person from being able to make use of an asset (legal negative control), and/or the right to obtain (from another person) the ability to make use of an asset (legal positive control), as we are purely looking at the factual position. It can also be distinguished from (2) control over a person’s behaviour (as we are looking at control over an *object*). Specifying this meaning from the outset would provide sufficient clarity.

In any event, the FCARs (and fixed charge) debate is something that has to be engaged with regardless of whether possession or control is used in the digital asset context.<sup>261</sup> Even if we say that a digital asset can be possessed, we would still have to determine what constitutes a sufficient degree of control over a digital asset to create a fixed charge, or what constitutes ‘possession or control’ of a digital asset that falls within the FCARs. These are not possession-dependent doctrines.

### ***3.3.3 Why not any other concept?***

At this point, it may still be objected that *another* concept is preferable to possession or control – it might be argued that a desert-based or utility-based criterion would be a better alternative. However, it is suggested that such desert or utility based tests would be undesirable. The main problem is that such tests are too difficult to apply, as they are too subjective, and this leads to substantially higher information costs and adjudication costs.

---

<sup>260</sup> Compare e.g. the examples provided in Vaudry and Green (n 18 above), 629-633.

<sup>261</sup> To the extent that the FCARs are applicable to digital assets (see e.g. Hin Liu and Louise Gullifer, ‘Financial collateral arrangements in the digital asset world’ (2022) 8 JIBFL 527).

As Crawford notes, the rules on the acquisition of title must adhere to the ‘simplicity imperative’, where the rule must be simple to apply.<sup>262</sup> A complex (or subjective) rule would lead to many inefficiencies since people would need to expend substantial time and cost to ascertain the legal position. Also, too many disputes would arise, since people have different interpretations of (e.g.) whether one has invested a ‘substantial’ amount of labour, or whether one has a sufficient ‘need’ for the asset. This increases adjudication costs, and creates the risk of a disagreeable society that may erupt into violence.

In addition, rules other than ‘possession’ or ‘control’ can be exploited by the parties, leading to a rule that is not ‘cheat-proof’.<sup>263</sup> If we adopt, for example, a ‘need-based’ rule, people would be able to cheat relatively easily as they can hide assets or declare them on trust in order to take advantage of the rule whereby they would be able to acquire title to an asset if they are able to demonstrate a greater ‘need’ for it. In contrast, with ‘possession’ or ‘control’, whether one has possession or control of an asset is an observable phenomenon, meaning that parties would not be able to take advantage of the rule – they would need to have the requisite degree of control (physical or otherwise) over the asset, and this control cannot be ‘faked’.

Furthermore, there is no analogy with ‘manufacture’ as a method of acquiring title.<sup>264</sup> Manufacture involves a situation where “a person takes materials and manufactures something new from them”,<sup>265</sup> with the result that the relevant person who ‘mixes’ the materials together obtains title to the new thing.<sup>266</sup> In the digital asset context, when one obtains control of a digital asset there is no act of mixing. The digital asset is either minted or mined into the relevant address controlled by the person, or it is transferred into such an address. There are no

---

<sup>262</sup> Crawford (n 18 above), 109-111. Crawford is discussing this point in relation to tangibles, but the same need for simplicity applies to digital assets because of information cost considerations and the need to respect market expectations (see Section 3.3.3 above).

<sup>263</sup> Crawford (n 18 above), 110-111.

<sup>264</sup> I.e. *specificatio* under Roman law

<sup>265</sup> Douglas (n 2 above), 29.

<sup>266</sup> *Borden (UK) Ltd v Scottish Timber Products Ltd* [1981] Ch 25. See also Institutes of Justinian Book 2 Title 1 para 25; Ernest Lorenzen, Specification in the Civil Law’ (1925) 35 Yale LJ 29; Law Commission, *Consultation paper* (n 8 above), 13.15.

‘prior existing ingredients’ that are mixed together to create the digital asset – in the case of minting, a new thing is created from scratch, and in the case of a transfer, an existing thing is transferred into the address (with nothing new being created).

#### **4. Conclusion**

This chapter has established that the threshold for obtaining a property right to a digital asset should be when someone obtains positive and negative control of a digital asset with the intention to exercise control over it on his own behalf. This threshold mirrors the ‘possession’ threshold for physical assets, and the underlying justifications for title apply to the same extent to digital assets as they do to physical assets.

However, we should not directly call this threshold ‘possession’ because this would mean that the concept of ‘possession’ would be extended to apply to digital assets. The possession jurisprudence would presumptively apply to digital assets, and this is undesirable because (1) bad rules will be replicated in the digital asset context, (2) the differences between physical and digital assets are likely to be obscured (or irrelevant differences may mistakenly be seen as significant), (3) there will be a ‘path-dependence’ that makes it difficult for judges to depart from possession jurisprudence, and (4) there will be undesirable practical consequences in the litigation context.

Instead, the concept of ‘control’ should be used. Control is a preferable concept to possession, primarily because there is no need to deal with a set of possession-dependent doctrines designed for physical assets. The aforementioned consequences would be avoided, and as long as the meaning of control in this context is specified and clarified, the law would not be rendered unacceptably uncertain. In this regard, the threshold of ‘factual positive and negative control’ is more than sufficient to point the way forward.

## **Chapter 3: Transferring the property right**

### **1. Introduction**

Chapter 2 explored the appropriate threshold for acquiring an original property right to a digital asset, and this chapter will explore the appropriate threshold for transferring such a property right to another person.<sup>1</sup>

Its primary focus is on exploring the various options for what the appropriate rule could be to transfer a property right to a digital asset in the *inter vivos* context, and will not discuss transfers of property rights by operation of law (such as in the bankruptcy, insolvency or succession contexts).<sup>2</sup>

There is some discussion of the transfer issue in the literature,<sup>3</sup> and the DIFC has introduced a legislative provision that governs the transfer of title to a digital asset.<sup>4</sup> However, the question of how to transfer legal title (as well as how to transfer a property right) to a digital asset has not been explored by the courts.

---

<sup>1</sup> Or technically, for transferring the property right *plus* the power to alienate the property right. I am proceeding on the assumption that there is a good normative case for recognising the power to alienate (and create a trust or charge over) the property right: see Chapter 1, Section 4.1.3, para 12 (final para) above).

<sup>2</sup> I will also not be discussing co-ownership.

<sup>3</sup> Law Commission of England and Wales, *Digital Assets: Consultation paper* (Law Com No 256, 2022), 13.17-13.22, 13.95-13.143; Law Commission of England and Wales, *Digital Assets: Final report* (HC 1486, Law Com No 412, 2023), 6.39-6.47; David Fox, 'Cryptocurrencies in the Common Law of Property' in S Green, D Fox, *Cryptocurrencies in Public and Private Law* (OUP, 2019) 6.48-6.51; Dubai International Financial Centre, *Consultation Paper No. 4 (September 2023) Digital Assets Law (2023)*, paras 62-82; Louise Gullifer, 'The private law of digital assets: what is it and what should it be?' 2021 Birkenhead Lecture, Gray's Inn, London (17 November 2021), at p 5 of lecture transcript:

<https://www.graysinn.org.uk/sites/default/files/documents/education/The%20private%20law%20of%20digital%20assets%2017.11%20-%20Birkenhead%20Lecture.pdf> (accessed 31 May 2024); Hin Liu, 'Transferring legal title to a digital asset' (2023) 5 JIBFL 317 ("Liu, 'Transfer Part 1'"); Hin Liu, 'Transferring legal title to a digital asset: shared and limited control arrangements (Part 2)' (2024) 4 JIBFL 251 ("Liu, 'Transfer Part 2'");

<sup>4</sup> The main provision that governs transfers of title is Article 12(1) of the DIFC's Digital Assets Law (DIFC Law No. 2 of 2024) ("DAL").

This question matters greatly because many issues depend on who has title (and thus by extension a property right)<sup>5</sup> to a digital asset at any given time. For example, in determining the question of whether someone is a bona fide purchaser of the *legal title*, we need to determine whether this person has acquired the legal title. Similarly, in the context of rescission, we need to determine whether the person against whom rescission is sought has acquired the legal title. In turn, in the context of interference, the regime adopted may be such that we need to determine whether the person seeking to sue for interference has or had legal title to the digital asset, for that could determine his entitlement to sue.<sup>6</sup>

This chapter will first set out the background context in relation to the transfer debate, (Sections 2-4) and then briefly discuss (and dismiss) the options of transferring a property right by deed and by agreement (Sections 5 and 6). It will then outline the rationale of the ‘delivery’ and ‘sale’ methods of transferring title to a physical asset (Section 7). Next, it will discuss the options of transferring a property right via a change of control (with an intention to transfer the property right), and via an on-chain transfer (with an intention to transfer the property right) (Sections 8 and 9). Finally, it will conclude (Section 10).

It is suggested that the appropriate requirement<sup>7</sup> should be that of ‘change of control’, with an intention on the part of the transferor<sup>8</sup> to transfer his property right to the transferee.<sup>9</sup> The precise threshold that constitutes a sufficient ‘change of control’, however, depends on

---

<sup>5</sup> For the purposes of this chapter, I will assume that (1) a transfer of the property right is sufficient to transfer the powers associated with such a right (and thus sufficient to transfer title), and (2) the powers associated with the property right cannot be transferred independently of the property right. I am making these two assumptions because the rights and powers cannot be held by separate people (since title is one ‘package’ and thus the rights and powers need to be held by the same person). Assumption 2 holds true for physical assets. As for Assumption 1, this is made because in practice, a person who intends to transfer their property right intends to transfer the entire ‘package’ of rights and powers (and thus intends to transfer title) – it is difficult to envisage a situation where one intends to transfer his property right without also intending to transfer the powers associated with it. Thus, for the purposes of Sections 8 and 9, an intention to transfer a property right is in practice equivalent to an intention to transfer title because having the former practically means having the latter. The two assumptions also simplify the analysis when discussing the ‘control-title’ inference (and people’s reliance on it).

<sup>6</sup> E.g. the regime under Article 14 of the DAL.

<sup>7</sup> I.e. the only way in which a property right should be transferred.

<sup>8</sup> I.e. the person with the property right who is looking to transfer his property right.

<sup>9</sup> I.e. the person to whom the transferor intends to transfer his property right.

which normative considerations to prioritise,<sup>10</sup> and there is no clear right answer as to what the threshold (and by extension, the appropriate rule or formulation) should be. There can be reasonable disagreement as to where the optimal balance should lie and which formulation is the most desirable.

Nonetheless, it is suggested that there is a three-stage approach that can be used to determine which rule to adopt. First, one needs to identify the normative considerations at play, and determine which ones are to be prioritised (and to what extent). Second, with the normative balance of considerations in mind, one needs to determine from an analytical perspective which concrete situations should be sufficient to transfer the property right, i.e. what the threshold should be. Third, the relevant threshold needs to be translated into a concrete rule that is linguistically formulated in a way that best captures or approximates such a threshold, and provides enough certainty and flexibility.<sup>11</sup>

This chapter will again draw comparisons with physical assets (and the rules governing the transfer of title to physical assets), and it is important to clarify where the analogies and distinctions lie in terms of ‘aim, substance and technique’. First, in both the physical and digital asset contexts, the aim is to ascertain the threshold that strikes the most appropriate balance between providing the transferor with enough autonomy and giving effect to the policy considerations relevant in imposing (or not imposing) a formality<sup>12</sup> rule.

Second, the substantive threshold to be adopted in terms of transferring a property right differs greatly between physical and digital assets, and thus there are some distinctions that are drawn (for example when discussing whether transferring a property right by agreement is

---

<sup>10</sup> And then, when the normative balance between the considerations is decided, one still needs to determine which shared and limited control arrangements should be sufficient to transfer title, and how best to produce a rule that best captures the intended threshold while providing enough flexibility and certainty.

<sup>11</sup> Flexibility is very important as the rule needs to accommodate new technological innovations and arrangements.

<sup>12</sup> E.g. deed, delivery, change of control, on-chain transfer.

appropriate). That said, some analogies will be drawn between physical and digital assets (for example, the similarity between delivery and change of control).<sup>13</sup>

Third, the techniques used to give effect to the relevant threshold for transferring a property right to a digital asset are very different to those in the physical asset context.

## 2. Clarification about ‘transfer’

Although this chapter’s focus is on the transfer of the *property right* to a digital asset, the notion of a ‘transfer’ is used very ambiguously in the blockchain context, and it is crucial to clarify what could be meant by a ‘transfer’. There are three main ways in which it is used, the first two of which denote a factual event, and the third referring to a legal event. The first way ‘transfer’ is used is to denote an on-chain transfer in respect of a digital asset such that it is now located at a different public address. The second notion of ‘transfer’ denotes a ‘change of control’ or a ‘transfer of control’, i.e. transferring control of a digital asset to another person (or group of people).<sup>14</sup> This can happen without an on-chain transfer, for example where a USB stick is handed to the transferee where the private key is stored inside the USB and the transferor has no knowledge of the key.<sup>15</sup> The final notion of transfer refers to the transfer of legal title (which, of course, encompasses the transfer of a property right).

The second meaning can be confused with the first meaning, since in both cases the holder of the private key is in the same factual position in respect of the digital asset, namely that he is the only person who has the power to execute an on-chain transfer of the digital asset.<sup>16</sup> It can also be lumped with the third meaning, since people make the general assumption

---

<sup>13</sup> To support a change of control requirement: see Section 8.1.3 below.

<sup>14</sup> Liu, ‘Transfer Part 1’ (n 3 above), 318.

<sup>15</sup> An example would be when an Opendime USB stick is handed over to the transferee.

<sup>16</sup> Subject to certain situations involving ‘shared control’ and ‘limited control’ (see Section 8.2, paras 2-3 below for meaning of ‘shared control’ and ‘limited control’).

that an action that changes the identity of the person who has exclusive control of a digital asset results in a transfer of title to a digital asset.<sup>17</sup>

The first and third meanings are often lumped together, because people may assume or expect that a change in the state of the blockchain also corresponds with a change to the location of title.<sup>18</sup> Thus, it is crucial to separate the meanings and examine how the three meanings interrelate.

This chapter explores the conditions required for the transfer of a property right (which is a subset of the third meaning of ‘transfer’). In particular, it discusses (*inter alia*) whether ‘change of control’ (the second meaning) and ‘on-chain transfer’ (the first meaning) are necessary or sufficient conditions for the transfer of a property right.

### **3. Transferring a property right: the policies**

When considering the appropriate rule to adopt in relation to transferring a property right to a digital asset, there are various policies to take into account – some that are general to any discussion of formality rules, and some that apply in particular to the blockchain context.

The general factors to take into account when considering whether to impose a formality rule (and if so, what type) have been encapsulated by McFarlane.

As McFarlane notes in *The Structure of Property Law*,<sup>19</sup> there are four reasons for imposing a formality requirement: evidence, reduction of fraudulent claims, publicity, and caution. First, a formality requirement provides evidence to the parties as to the existence of the relevant transaction. Second, it reduces the chance of third parties fraudulently asserting

---

<sup>17</sup> This follows from the general ‘control-title’ inference: see Section 3.1 below.

<sup>18</sup> In addition to the general ‘control-title’ inference (see Section 3.1 below), people may make the further assumption that a change in the state of the ledger corresponds with a change in the identity of the person in control.

<sup>19</sup> Ben McFarlane, *The Structure of Property Law* (Hart Publishing, 2008), 104-110.

that a person with legal title to an asset has transferred a right or granted an interest to them,<sup>20</sup> as the third party in question would need to prove that the formality requirement was satisfied (e.g. that there was delivery, writing, or a deed).<sup>21</sup> With these formality requirements, the third party would gain nothing from fabricating a claim that (for example) the owner orally agreed to sell the asset to him. Third, formalities such as registration provide publicity to third parties, by providing notice that the transferee has the relevant right or interest, as they can simply search the relevant source (such as the register) to find this out.<sup>22</sup> Fourth, formalities have a cautionary effect on transferors as they are forced to think seriously about the transfer, and this ensures that ‘oral transfers’ conducted on a whim will not have legal effect.

Opposed to these four reasons, there are several reasons against the imposition of a formality requirement. The first is the inconvenience and expense involved in complying with a particular formality requirement: the need to have a deed (or writing), or the need to register, takes time and/or money. Second, imposing a formality requirement may frustrate reasonable expectations or cause unfair surprise. If in a particular context it is (for example) customary or normal market practice to conduct transactions orally, imposing a formality requirement of writing would cause unfair surprise to people in that context as they find out that their transactions are void or unenforceable for a lack of writing. Third, there may be vagueness in (1) the scope of the rule and/or (2) what satisfies the formality requirement, making the rule difficult to apply. This also creates the further consequence that judges may (for pragmatic

---

<sup>20</sup> McFarlane focuses on the risk of fraudulent claims against the legal title holder (“A”), but the ‘prevention of fraudulent conduct’ point applies more generally. For example, it would apply to the ‘double sale’ situation where the fraud is perpetrated by the legal title holder: see Section 3.3 below.

<sup>21</sup> In the case of a deed for example, they would not be able to do so without fabricating the relevant document containing the necessary content and signatures, and even in that case they would be risking serious criminal consequences: see McFarlane (n 19 above), 105-106.

<sup>22</sup> Or where there is a ‘delivery’ formality requirement, the transferor’s lack of possession acts as ‘negative publicity’, in that a third party can observe that the item is not in the possession of the transferor and make the general assumption that he does not have title.

reasons) resort to unnatural interpretations of the requirement to reach reasonable outcomes, which may in turn render the law uncertain, technical and/or complex.<sup>23</sup>

Ultimately, when deciding whether to impose a formality requirement in a particular context, we need to assess the relative weight of the reasons for and the reasons against imposing such a requirement. In the blockchain context, there are certain context-specific policies that are particularly relevant.

### **3.1 The control-title inference and decoupling**

As mentioned in Chapter 2,<sup>24</sup> one of the core purposes of the blockchain is to allow people to store and move value in an efficient and safe way without the need for a central counterparty or intermediary, and this is achieved through creating ‘locked virtual spaces’ (addresses) over which people can have exclusive control, and a ledger in which movements of assets between these ‘spaces’ are recorded.<sup>25</sup>

The creation of this ecosystem leads people to make assumptions, and the crucial assumption people make is the ‘control-title’ inference – namely that if someone has control of one of these ‘spaces’ then he has (legal) title to assets in such a ‘space’. In other words, people make the general inference or assumption that when someone has control of a digital asset, he has title to it.<sup>26</sup>

---

<sup>23</sup> McFarlane raises the issues of (1) “an increase in technicality and complexity” and (2) “a lack of transparency in the law”: see McFarlane (n 19 above), 107-108.

<sup>24</sup> Chapter 2, Section 2.2.3 above.

<sup>25</sup> Liu, ‘Transfer Part 1’ (n 3 above), 317.

<sup>26</sup> There is of course the question of what degree of control triggers the control-title inference. The core case is where the person has the only key in a single-signature address, or all the keys in a multi-signature address. If there is a lower degree of control (e.g. having positive and/or negative control without having all the keys), some might make the control-title inference but others would not. Whether a person does so also depends on how the blockchain protocol is configured or programmed, as various protocols do not reveal whether an address is a single-signature or a multi-signature address.

This mirrors the general inference people make in the physical asset context that if someone has possession of a physical asset, he has title to it. This assumption<sup>27</sup> is made as a default psychological heuristic that reflects people's general experience.<sup>28</sup>

As a result, it is important in the blockchain context not to have too much 'decoupling' between control and title. This is because such 'decoupling' means that loss may be caused to purchasers and creditors who act on the assumption that a party with control has title. This defeats their reasonable expectations.

### **3.2 Frustration of reasonable expectations: Purchasers and creditors**

In relation to purchasers, they expect that a seller who has control<sup>29</sup> of a digital asset has title to it, even if the seller does not. In such a case, the purchaser would assume that when control is transferred to him, he would have title to it as well. Here, in the absence of a 'general' bona fide purchase rule, the purchaser would not always obtain (the best) title to the digital asset, and to this extent the purchaser's reasonable expectation would be defeated.<sup>30</sup>

In relation to creditors, they may make lending decisions that are based on false assumptions about a person's wealth. Because of the control-title inference, a creditor may falsely believe that a person who controls a digital asset and represents that he owns it actually does own it, and such creditor may (for example) make a loan secured over the digital asset.

In such a situation, the creditor would expect to be able to have priority when enforcing the debt against the asset. His expectation would therefore be defeated when he discovers he

---

<sup>27</sup> Liu, 'Transfer Part 1' (n 3 above), 320.

<sup>28</sup> See also discussion in Michael Crawford, *An Expressive Theory of Possession* (Hart Publishing, 2020), Chapters 3 and 4.

<sup>29</sup> At least in the case where the seller has all the keys to the address.

<sup>30</sup> In addition to purchasers, donees would also have their expectations defeated as well, if they receive control of an asset from a transferor.

does not have such priority, and (if he sells the asset nonetheless) may also face liability for interference with the digital asset.<sup>31</sup>

Thus, the policy of preventing the frustration of reasonable expectations as a result of the ‘control-title inference’ means that there needs to be a baseline degree of coupling between control and title.

### **3.3 Risk of fraud and misappropriation**

Apart from the frustration of reasonable expectations, there is also the need to limit the risks of fraud and misappropriation.

One type of fraud would be where a person (X) fraudulently asserts that the owner (Y) of a digital asset transferred title to him by way of an oral agreement. In the absence of a formality requirement (such as a change of control), Y may well need to defend X’s claim in court. In contrast, if there is a formality requirement such as a change of control, Y has a cast-iron defence<sup>32</sup> based on the fact that there has (for example) been no change of control<sup>33</sup> and thus no transfer of title.

Another type of fraud is the ‘double sale’, which happens where the seller (X) can transfer title to a digital asset without any change of control. For example, X could sell his digital asset to Y by agreement while retaining control over it (e.g. in his single-sig address) and then represent to Z that he still owns the asset, given that Z would generally make the ‘control-title’ inference.<sup>34</sup> If X ‘sells’ the asset (for a second time) to Z and transfers control of

---

<sup>31</sup> Liu, ‘Transfer Part 2’ (n 3 above), 253. However, there would be no liability under the impairment tort proposed in Chapter 4 as the mental requirement (intention or recklessness) would not be satisfied: see Chapter 4, Section 4.1.2.

<sup>32</sup> McFarlane (n 19 above), 105.

<sup>33</sup> If a ‘change of control’ requirement to transfer title is adopted.

<sup>34</sup> The ‘single sig’ situation would be a ‘core case’ where the control-title inference is engaged.

it to Z, the bona fide purchase rule may extinguish Y's title.<sup>35</sup> Alternatively, if there is no applicable bona fide purchase rule, Z would not obtain a clean title but rather take subject to Y's title. In either case, either Y or Z would be unjustifiably prejudiced,<sup>36</sup> and X profits twice.

Also, there is a risk of misappropriation where control of a digital asset is shared. If the law allows title to be transferred in situations where there is a change of control but the transferee shares control with another person, there is a risk that the other person would unilaterally misappropriate the asset. For example, where the transferee (Y) and another person (X) each have one key in the 1 of 2 multisig<sup>37</sup> wallet in which the digital asset is held, X could unilaterally misappropriate the digital asset and thus deprive Y of control of the digital asset, given that in this example one key is sufficient to execute a blockchain transaction.

### **3.4 Party autonomy**

The above factors limit the degree of party autonomy, so the question arises as to what reasons militate in favour of providing a higher degree of party autonomy despite the concerns mentioned above. There are two main reasons.

First, providing a higher degree of party autonomy would encourage the use of new technological innovations in this nascent industry with arguably a lot of (actual and potential) use cases.<sup>38</sup> Second, insofar as people reasonably expect title to be transferred in a particular situation (and especially if there is an established market practice), imposing an overly

---

<sup>35</sup> In the case that there is an applicable bona fide purchase ("BFP") rule.

<sup>36</sup> Also, if there is no BFP rule, Y may also be factually prejudiced if he has to sue to recover the asset (or its value) from Z, insofar as that may be more difficult than doing so (or otherwise recovering control of the asset) from X.

<sup>37</sup> Multi-signature. A 'X of Y multisig' arrangement denotes an arrangement where there are Y keys and a signature from X keys are required to sign a transaction.

<sup>38</sup> Such as in the context of digital securities and investment, collective decision making structures, electronic trade documents, succession, and smart contracts.

restrictive formality requirement would defeat such expectations in relation to when title ought to be transferred, and run counter to market practice.<sup>39</sup>

#### 4. Ways of transferring a property right: the options

A digital asset is not a right against a person, but rather an object that is independent of the legal system. As such, a property right to a digital asset cannot be transferred by assignment or novation because only rights against persons<sup>40</sup> can be transferred by assignment or novation.

Digital assets are more analogous to chattels given they are things independent of the legal system, and rivalrous,<sup>41</sup> and so the methods of transferring legal title to a chattel (deed, agreement (sale), and delivery) have more relevance to digital assets.

The ‘deed’ and ‘agreement’ methods have been mentioned in the context of digital assets, but the general academic and market consensus is that they are undesirable methods to transfer title<sup>42</sup> (and thus a property right). What has been discussed the most and is favoured by a number of academics and market participants is a requirement of a ‘change of control’,<sup>43</sup> which is similar to the delivery of a chattel.<sup>44</sup> There is also the option of an ‘on-chain transfer’ requirement, which also has certain similarities to the delivery of a chattel.<sup>45</sup>

---

<sup>39</sup> It is important to note that giving effect to the reasonable expectations of parties can support a more relaxed formality rule (and not just a more restrictive one), given that different reasonable expectations can arise in different situations.

<sup>40</sup> And possibly Hohfeldian liberties such as milk quotas and carbon emission allowances, which digital assets are not.

<sup>41</sup> See e.g. Law Commission, *Final report* (n 3 above), 4.22-4.47.

<sup>42</sup> See e.g. Gullifer (n 3 above), p.4; Law Commission, *Consultation paper* (n 3 above), 13.130-13.140; Liu, ‘Transfer Part 1’ (n 3 above), 319 and 320-321.

<sup>43</sup> Law Commission, *Final report* (n 3 above), 6.39-6.47; DIFC, *Consultation paper* (n 3 above), paras 62-82.

<sup>44</sup> Gullifer (n 3 above), 5.

<sup>45</sup> The movement of a digital asset from ‘space’ to ‘space’ via-an on chain transfer is (at least for the situations involving a change of control) similar to the paradigm case of delivery, where physical goods are transported from the transferor’s ‘space’ to the transferee’s ‘space’.

The four options (deed, agreement, change of control, and on chain transfer) will be explored in Sections 5, 7, 8 and 9 respectively.<sup>46</sup> The first option is to transfer a property right by deed, which will now be discussed.

## 5. Deed

Using a deed is one of the ways in which title to a chattel can be transferred.<sup>47</sup> Although there is no explicit discussion in the case law about the rationale of the deed requirement in the context of transferring title to chattels, there are various benefits to imposing a deed requirement. First, it provides evidence of a transaction between the parties and aids in preventing fraud. For example, if one party wishes to deny that the transaction took place, the other party can use the deed as evidence and thereby disprove such allegations. Second, imposing a deed requirement produces a cautionary effect for the transferor, as the act of producing and signing a formal document in front of witness(es)<sup>48</sup> will go towards ensuring that the transferor's intention to enter into the transaction is not a mere product of haste, but instead seriously contemplated with the relevant consequences in mind.

However, there are two obvious disadvantages of the deed method. First, having a document drawn up and signed in the presence of witness(es) just to transfer title to a chattel is extremely unwieldy. Second, a deed provides no publicity to third parties, such that they would not be able to reliably infer who has title merely based on who possesses the chattel, since someone may possess a chattel but not have title to it because they used a deed to transfer title.

---

<sup>46</sup> Section 6 will discuss the rationale of the 'delivery' and 'sale' requirements for transferring title to a physical asset, in order to contextualise the discussion at Sections 7, 8 and 9.

<sup>47</sup> *Cochrane v Moore* (1890) 25 QBD 57, 65-72; Michael Bridge, Louise Gullifer, Kelvin Low, Gerard McMeel, *The Law of Personal Property* (3<sup>rd</sup> edition, Sweet and Maxwell 2021). 18-007.

<sup>48</sup> Bridge et al (n 47 above), 18-009 (discussing the requirements under ss.1(2)-1(3) of the Law of Property (Miscellaneous Provisions) Act 1989).

In the digital asset context, allowing a deed to be sufficient to transfer a property right would be disastrous. Transferring a property right by way of deed would mean that such a right can be transferred off-chain without a change of control (thus freely decoupling title and control). This in turn gives rise to the ‘double sale’ problem, where (in this context) A sells a digital asset to B by way of deed without transferring control of the asset,<sup>49</sup> and then (fraudulently) sells the asset to C through transferring control of the asset to C. In this case, B or C would be prejudiced.<sup>50</sup> Apart from the ‘double sale’ problem, there is also no safeguard against the situation where the creditor lends against a person who has control of a digital asset (in this case A) but no title to it and is prejudiced as a result.<sup>51</sup>

Also, insofar as the deed method in the physical asset context was underpinned by the need to eliminate the need to physically deliver a heavy or bulky object, this concern is not applicable to digital assets because digital assets are ‘moved around the digital space’ by way of an on-chain transfer instead of physical acts that can be laborious.

*Requiring* a deed for a property right to be transferred is even more disastrous. Apart from the above disadvantages, this causes a massive inconvenience: one cannot transfer a property right to a digital asset by executing an on-chain transfer. For example, a deed requirement would prevent A’s property right from being transferred to B even where there is (e.g.) an on-chain transfer that completely changes control from A to B (without the use of a deed). A still has the property right, while B has control. This decouples control and title, defeats the parties’ expectations and creates an absurd result that discourages people from using the blockchain mechanism itself to transfer their property right(s).<sup>52</sup>

---

<sup>49</sup> The crucial fact is that the initial sale to B happens without change of control to B.

<sup>50</sup> Either C obtains a title that is inferior to B’s (where there is no BFP rule), or B’s title is extinguished by C purchasing the asset and obtaining control (where there is a BFP rule). See Section 3.3, para 3 above.

<sup>51</sup> See Section 3.2 above.

<sup>52</sup> This outcome defeats a core purpose of the blockchain, specifically its role as a facilitative mechanism that provides a way to quickly change the person who has control of a digital asset via an on-chain transfer and thereby transfer one’s property right(s).

In addition, just as in the physical asset context, a deed provides no publicity. This stands in contrast with an on-chain transfer (which provides positive publicity),<sup>53</sup> or an off-chain change of control, which provides some negative publicity in that a third party will know that the relevant person does not have control of the asset, given that he cannot sign a signature from the address in which the asset is contained.<sup>54</sup>

## 6. Delivery and sale: the rationales

Having established that using a deed as a method of (or requirement for) transferring a property right is inappropriate in the digital asset context, it would be apposite to explore the rationales behind the delivery and sale methods of transferring title (in respect of physical assets), and examine whether they apply across to digital assets when considering the ‘agreement’, ‘change of control’, and ‘on-chain transfer’<sup>55</sup> methods of transferring a property right to a digital asset.

Stripped to its essence, delivery involves the transferee acquiring possession of a physical asset with the consent of the transferor.<sup>56</sup> The case law on the delivery requirement for physical assets does not discuss the rationale of this requirement in much detail.<sup>57</sup> There have been several rationales for the delivery rule that are incorrect or circular, such as ‘delivery is part of the definition of a gift’<sup>58</sup> or ‘it is normal to deliver the goods where there is a gift’.<sup>59</sup> The first is circular because it does not show why ‘giving and taking’ should be imposed as a

---

<sup>53</sup> An on-chain transfer publicises a change in the location of the digital asset.

<sup>54</sup> Without the private key, he cannot sign a digital signature from the address at which the asset is located.

<sup>55</sup> There are similarities between ‘delivery’ and ‘change of control’ (see Section 8.1.3 below), and between ‘delivery’ and ‘on-chain transfer (albeit to a lesser extent: see n 45 above).

<sup>56</sup> See e.g. *Thomas v Times Book Co Ltd* [1966] 2 All ER 241.

<sup>57</sup> Samuel Stoljar, ‘The Delivery of Chattels’ (1958) 21 MLR 27.

<sup>58</sup> *Cochrane* (n 47 above), 75-76; Stoljar (n 57 above), 29.

<sup>59</sup> Stoljar (n 57 above), 29, citing Mechem, ‘The Requirement of Delivery in Gifts of Chattels and of Choses in Action Evidenced by Commercial Instruments’ (1926-1927) 21 Illinois L.R. 341, 457, 568.

requirement for transferring legal title. Similarly, the second also does not explain why delivery should be a *requirement* for transferring title to a physical asset.<sup>60</sup>

Nonetheless, the delivery requirement for physical assets can be rationalised as a manifestation of the basic principle that ‘possession is evidence of title’. Generally, we make the assumption that a person who has possession of a physical asset has title to it, and the delivery rule helps us track this assumption by aligning possession with title insofar as it ensures that without a transfer of possession, there is no transfer of title. As such, the ‘publicity’ and ‘evidence’ functions can be fulfilled. The disadvantage of a delivery requirement (as with a deed requirement) is the inconvenience and expense involved.

With the introduction of the *indebitatus assumpsit* and the rise of consensual contracts,<sup>61</sup> the law developed such that title could be transferred (under a sale) by way of agreement.<sup>62</sup> This was later codified in the form of Section 17 of the Sale of Goods Act 1979. It provides that property in specific or ascertained goods can pass when the parties intend it to pass (i.e. when they agree),<sup>63</sup> and so there is no need for any act of delivery.

Indeed, this transition was fuelled by the commercial convenience of not having to wait for the goods to be shipped halfway across the world, or having to use a deed, for title to be transferred. Party autonomy and commercial convenience<sup>64</sup> therefore underpin the rule that agreement is sufficient to transfer title to goods under a sale. The balance struck by the rule indicates a preference for convenience over the corresponding increase in the risk of fraud, or the decrease in publicity/reduced signalling effects. The latter concerns are partially mitigated

---

<sup>60</sup> Promises that are sincerely intended (non-jocular) do not necessarily have to involve delivery: see Stoljar (n 57 above), 29.

<sup>61</sup> *Cochrane* (n 47 above), 70-71.

<sup>62</sup> See e.g. David Ibbetson, ‘Sale of goods in the fourteenth century’ (1991) 107 LQR 480.

<sup>63</sup> For the agreement to be a contract of sale of goods, to which s 17 can apply, it must be a contract “by which the seller transfers or agrees to transfer the property in goods to the buyer for a money consideration”: SGA s. 2(1).

<sup>64</sup> McFarlane (n 19 above), 177.

through the introduction of *nemo dat* exceptions that offer protection to a bona fide purchaser in specified circumstances.<sup>65</sup>

## 7. Agreement

The second possibility is to allow a property right to a digital asset to be transferred where the parties agree. This would be analogous to the position in respect of chattels where s.17 of the Sale of Goods Act 1979 (“SGA”) allows title (and thus a property right) to pass by agreement.<sup>66</sup> Just like a chattel, a digital asset is a ‘thing’ independent of the legal system, and so it is worth considering whether the situation in the digital asset context is sufficiently analogous to the chattel context such that a similar transfer rule<sup>67</sup> should be applied.

The advantage of allowing a property right to pass by agreement is that it enhances party autonomy. By dispensing with the need for any formality requirement, it becomes easier for parties to transfer a property right to a digital asset (they can just agree to do so). However, this also brings in all the disadvantages of *not* having a formality requirement, particularly in relation to the risk of fraud, and the frustration of reasonable expectations (unfair surprise).

Commentators have been against the idea that title (and thus a property right)<sup>68</sup> to a digital asset can pass by agreement.<sup>69</sup> The main reason is that this would cause control and title to be decoupled at will (given that title can pass with absolutely *no* change of control),<sup>70</sup> which increases the risk of fraud and defeats parties’ expectations.

---

<sup>65</sup> SGA ss.21-25, and Factors Act s.2(1).

<sup>66</sup> Provided there is money consideration (see definition of contract of sale in SGA s.2(1)), and that the goods are specific or ascertained (see SGA s17).

<sup>67</sup> Transfer rule’ i.e. the rule governing the transfer of a property right to a digital asset.

<sup>68</sup> Given the two assumptions made in n 5 above for the purposes of this chapter.

<sup>69</sup> See e.g. Gullifer (n 3 above) p.4; Liu, ‘Transfer Part 1’ (n 3 above), 320-321; Law Commission, *Consultation paper* (n 3 above), 13.133-13.140 (inappropriate analogy with tangibles and poor fit with statutes).

<sup>70</sup> See e.g. Gullifer (n 3 above) p.4; Liu, ‘Transfer Part 1’ (n 3 above), 320-321.

Allowing a property right to a digital asset to pass by agreement would freely give rise to many of the undesirable situations described earlier in Sections 3.2 and 3.3. Three of them are particularly relevant: (1) fraudulent assertions by a third party (Y) that the owner (X) transferred title<sup>71</sup> to him by agreement (which X may not be able to readily or immediately defend),<sup>72</sup> (2) ‘double sale’ frauds, and (3) creditors extending loans that are ‘apparently secured’ over digital assets that they are misled to believe are owned by the person in control. There is simply no safeguard against these three situations if a property right can pass by agreement.

One may nonetheless argue these risks may not be fatal because in the physical asset context, this decoupling is explicitly allowed by the SGA in permitting title to be transferred by agreement.<sup>73</sup> However, there is a key difference between physical goods and digital assets, such that the equivalent of a ‘sale’ rule (where title (and thus a property right) can pass as long as the parties agree) should not be introduced in the digital asset context. Specifically, the gain in commercial convenience by allowing a property right to pass by agreement is extremely significant for physical goods, whereas it is not for digital assets, such that this small advantage does not justify a departure from the formality rule.

In the physical goods context, goods need to be shipped from across the world (which could take months), and it would be inconvenient to require delivery (and hence change of control) of the goods for title to pass.<sup>74</sup> The buyer may want to use the goods to raise finance in the interim period between agreeing to buy and actual delivery, and so preventing title from passing (despite an agreement to buy the goods) will prevent the buyer from doing so (leading to an inefficient use of capital).

---

<sup>71</sup> And thus a property right: see n 68 above and text thereto.

<sup>72</sup> There would be no ‘cast-iron’ defence available to X: contrast n 32 above and text thereto.

<sup>73</sup> SGA, s.17.

<sup>74</sup> Similarly, with a deed requirement, a deed would need to be drawn up and signed in front of witnesses, which involves considerable inconvenience and expense.

This significant gain in commercial convenience, in allowing title to pass instantly by agreement instead of taking (potentially) months,<sup>75</sup> meant that the increased risks of fraud and defeating parties' reasonable expectations could on balance be tolerated.<sup>76</sup>

There is no corresponding benefit to permitting a property right to a digital asset to be transferred by agreement. Unlike with transferring control of a physical asset, transferring control of a digital asset can happen almost instantly, whether on-chain or off-chain. An on-chain change of control just requires one to interact with an existing application that connects to the blockchain<sup>77</sup> which would allow the transfer to happen. In turn, an off-chain change of control can be executed by way of a USB change of control,<sup>78</sup> which (if the parties are physically proximate enough) would be extremely convenient, and this is often preferable to an on-chain change of control because gas fees<sup>79</sup> do not need to be paid.<sup>80</sup>

Thus, dropping a 'change of control' type requirement<sup>81</sup> in the digital asset context in order to allow a property right to a digital asset to be transferred via agreement alone does not yield nearly the same gain in commercial convenience as compared to in the physical asset context. Given that there is no such gain, the increased fraud and decoupling risks that result from allowing title to a digital asset to pass on agreement would appear to be unjustified.<sup>82</sup>

## 8. Change of control

---

<sup>75</sup> Or needing to draw up a deed and sign it in front of witnesses.

<sup>76</sup> Liu, 'Transfer Part 1' (n 3 above), 320.

<sup>77</sup> E.g. MetaMask.

<sup>78</sup> See Section 2 above. An off-chain change of control can also be achieved using any other device that allows the transferor to divest himself of all control of the private key.

<sup>79</sup> I.e. blockchain transaction fees.

<sup>80</sup> See n 157 below and text thereto.

<sup>81</sup> I.e. a requirement broadly analogous to that of 'delivery' in the physical asset context.

<sup>82</sup> Liu, 'Transfer Part 1' (n 3 above), 319-321. A BFP rule would also not solve the problems arising from allowing title to a digital asset to pass by agreement: 321.

The next option is to impose a ‘change of control’ requirement for transferring legal title to a digital asset, and it is suggested that this option should be adopted.

### 8.1 The ‘change of control’ requirement and its benefits

‘Change of control’ is the requirement that has been discussed most and is favoured by a number of academics and market participants.<sup>83</sup>

Also, it has been adopted by the DIFC in the DAL.<sup>84</sup> Similarly, the Law Commission in their Final Report recommended that title should be transferred only when there is a ‘change of control’ coupled with the relevant intention.<sup>85</sup>

A ‘change of control’ involves the transferee obtaining control of the digital asset, either from the transferor, or from another person<sup>86</sup> or mechanism.<sup>87</sup> This, coupled with a mental element that the transferor intends to transfer his property right to the transferee,<sup>88</sup> should be the requirement for transferring a property right to a digital asset.

In practice, ‘change of control’ is a relatively easy requirement to satisfy, and can generally be done in seconds or minutes. As stated earlier,<sup>89</sup> a change of control can happen on-chain (via an on-chain transfer of the asset) or off-chain (via e.g. the physical transfer of a USB device where the private key is sealed, or a Layer 2 mechanism). As such, this is a relatively light formality requirement that causes relatively minimal inconvenience or expense.

---

<sup>83</sup> See e.g. Law Commission of England and Wales, *Digital assets Responses to consultation* (2022), 516, 525 (City of London Law Society), 770, 748 (Linklaters), 545-546 (Financial Markets Law Committee), 451 (Deloitte Legal (UK) – preference for ‘change of control’ over on-chain transfer); Gullifer (n 3 above), 5; Law Commission of England and Wales, *Digital assets Responses to the call for evidence* (2021), 22 (Louise Gullifer and David Fox – factual control as necessary condition); Law Commission, *Final report* (n 3 above), 6.41 and 6.39-6.47; DIFC, *Consultation paper* (n 3 above), paras 62-82; Liu, ‘Transfer Part 1’ (n 3 above).

<sup>84</sup> DAL, Article 12.

<sup>85</sup> Law Commission, *Final report* (n 3 above), 6.39-6.47.

<sup>86</sup> E.g. where the transferor’s digital asset is in the control of a custodian, and the transferor directs the custodian to transfer control of the digital asset to the transferee.

<sup>87</sup> E.g. where the transferee obtains control of the digital asset via a smart contract function.

<sup>88</sup> See Section 8.1.4 below.

<sup>89</sup> See Section 7 above (text to nn 76-80 above).

It is suggested that the crucial advantage of having a ‘change of control’ requirement is that it the best way of reflecting the policy against overly decoupling title and control. In imposing a ‘change of control’ requirement, the law directly defines the threshold in terms of control, and thus directly (and considerably) increases the degree of alignment between control and title. This therefore reduces the instances in which a party can fraudulently represent to a purchaser or creditor that he has title<sup>90</sup> to an asset,<sup>91</sup> and reduces the instances in which people would otherwise be misled as a result of making the control-title inference. Another advantage of a ‘change of control’ requirement, in contrast with an ‘agreement’ approach, is that it prevents people from fraudulently asserting a transfer of title when there has been no change of control.

These two benefits (coupled with the minimal inconvenience involved in effecting a change of control) are the reason why ‘change of control’ should be the general requirement for transferring a property right to a digital asset. The two benefits will be explored in turn.

### ***8.1.1 Less room to fraudulently represent, and less room to be misled by control-title inference***

Unlike the ‘deed’ and ‘agreement’ methods, having a ‘change of control’ requirement would significantly reduce the number of situations in which a party (X) can fraudulently represent to a purchaser or creditor that he owns the asset by retaining control of it.

Most crucially, it significantly reduces the situations in which X is able to conduct a ‘double sale’. If a change of control is required, X cannot sell a digital asset to Y via an oral agreement or a deed (while retaining positive and negative control) and then sell the asset again

---

<sup>90</sup> Specifically the best title.

<sup>91</sup> And by extension a property right to it.

to Z by fraudulently representing to Z that he still has title to the asset. As neither an oral agreement nor a deed is sufficient to transfer title, the ‘first sale’ to Y simply cannot occur. Also, if the change of control requirement requires the transferor (X)<sup>92</sup> to lose positive control,<sup>93</sup> then a double sale cannot be conducted because X will have divested himself of control during the first sale, and thus cannot represent to Z that he has title to the asset (based on his control) and sell it again.<sup>94</sup> Similarly (and by the same logic), if Z is a creditor instead of a purchaser, having a change of control requirement also significantly reduces the situations in which X can fraudulently represent to Z that he owns the asset and thus induce Z to extend a larger loan.

More generally, in terms of publicity, imposing a ‘change of control’ requirement helps to prevent third parties who want to buy or lend against a digital asset from being misled, regardless of whether there has been fraud. Requiring a change of control for the transfer of a property right to a digital asset means that (all else being equal) there will be fewer situations in which control and title are decoupled. Thus, if a purchaser agrees to buy an asset in a particular address and the seller changes control of the asset to the purchaser,<sup>95</sup> there is a much higher chance that the seller had good title to the asset immediately prior to the sale, and thus a much higher chance that the purchaser will obtain good title to the digital asset.<sup>96</sup> Similarly, if a secured creditor wants to lend against a digital asset in a particular address, there will be a much higher chance that the person who controls that address has title to the asset.

---

<sup>92</sup> Insofar as he has control to begin with.

<sup>93</sup> Positive factual control. The precise threshold that satisfies the ‘change of control’ requirement is an open question: see Section 8.2 below.

<sup>94</sup> Unless the transferor subsequently regains control of the asset.

<sup>95</sup> Under an agreement for immediate transfer of title upon the change of control, as opposed to an agreement for the transfer of title at a later time.

<sup>96</sup> The ‘all else being equal’ caveat is important here, because the Law Commission is recommending a ‘general’ bona fide purchaser rule that applies to all crypto-tokens (see Law Commission, *Consultation paper* (n 3 above), 13.84 and 13.50-13.90). If this rule is introduced, the purchaser will get a clean title anyway as long as he is a bona fide purchaser, regardless of whether the transferor had clean title. Ultimately, the extent to which a purchaser will obtain a clean title depends on the width of the relevant bona fide purchaser rule that is introduced.

Thus, having a ‘change of control’ requirement would significantly reduce the harms that arise from making the control-title inference and acting on it (when the person in control does not have title). By having more coupling (relative to a deed or an agreement requirement), there is less room for parties to be in situations where they have control but not title and abuse the fact that others make (and act on) the control-title inference. Crucially, having a ‘change of control’ requirement is the most direct way of giving effect to the policy of preventing too much decoupling and thus reduces the circumstances under which people can be misled by the control-title inference.

### ***8.1.2 Preventing fraudulent assertion and denial where no change of control***

There are also two further ways in which fraud is reduced from having a ‘change of control’ requirement as opposed to an ‘agreement’ requirement.

First, a third party cannot just fraudulently assert that the person in control transferred title to him via an oral agreement – to make the assertion of a title transfer believable, he would need to prove that he has obtained control of the digital asset. Second, the person in control cannot fraudulently *deny* a transfer of title in situations where there is no change of control. A ‘change of control’ requirement prevents the situation where the person in control (X) can sell the asset to Y via an oral agreement without any change of control, and fraudulently deny that the sale happened, with the result that Y cannot make out a good case that he has title to the asset because the asset is in X’s address, This situation is prevented because the sale cannot happen where there has been no change of control.

### ***8.1.3 Similarity with delivery***

It is helpful to point out a crucial similarity between the change of control of a digital asset and the delivery of a physical asset. Namely, that both involve the transferee acquiring control of the (digital or physical) asset).<sup>97</sup>

Thus, insofar as the rationale of the original ‘delivery’ requirement for transferring title to a physical asset is that it increases alignment between possession and title and thus reduces the instances of fraud,<sup>98</sup> this rationale is also applicable in the digital asset context. A change of control requirement for transferring a property right, just like a delivery requirement for transferring title, achieves this increased alignment by requiring the transferee to obtain control before he can acquire a property right (and thereby acquire title)<sup>99</sup> to a digital asset.

Also, insofar as a ‘delivery’ requirement prevents people who do not have possession from being able to fraudulently assert or deny that title has been transferred to them (because they would need to have to have possession to represent that title has been transferred to them), this is also achieved via a ‘change of control’ requirement. As stated earlier,<sup>100</sup> a person without control of a digital asset would not be able to credibly represent that he has title to a digital asset if there is a ‘change of control’ requirement.

#### ***8.1.4 Mental element***

Of course, the ‘change of control’ requirement comes with a requirement that the transferor intend to transfer his property right to the transferee.<sup>101</sup> If an intention requirement did not exist,

---

<sup>97</sup> See Section 6 above (text to n 57).

<sup>98</sup> Liu, ‘Transfer Part 1’ (n 3 above), 319; see also Section 6, para 3 above.

<sup>99</sup> See assumptions made at n 5 above.

<sup>100</sup> See Section 8.1.2 above.

<sup>101</sup> In the chattels context, there is also a question of whether ‘intent’ encompasses a requirement that the transferee agrees to the transfer (see e.g. Robert Stevens, *The Laws of Restitution* (OUP, 2023) 197); cf *Standing v Bowring* (1885) 31 Ch D 282, 288 (property vests in the transferee before he knows of the transfer, but he has the right to repudiate the transfer when informed of it); Bridge et al (n 47 above), 18-013 (donee presumed to accept gift unless he expressly repudiates it). This chapter is not concerned about this debate as its main focus is on the conduct element required on the part of the transferor (i.e. change of control, on chain transfer, etc) that is additional to intention.

the autonomy of the transferor simply would not be given effect to, as (e.g.) a person who hacks into the transferor's address could transfer the transferor's property right to himself, by procuring an unauthorised transfer of a digital asset into his own address.<sup>102</sup>

## 8.2 How much control?

The main debate in relation to the 'change of control' requirement relates to how much control the transferee needs to obtain before the requirement is satisfied. For example, would the transferee need to have the private key in a single sig address (or all the private keys in a multisig address), or would it be sufficient to have 2 keys in a 2 of 3 multisig address, or even one key in a 2 of 3 multisig address? This issue carries immense practical significance because there are many 'shared control' and 'limited control' scenarios in the digital asset industry.

'Shared control' scenarios involve situations in which multiple parties collectively have factual positive and negative control of a digital asset, but such control is shared such that at least one person does not have positive and negative control. These situations include multi-signature ('multisig') arrangements that involve multiple keys being held by different people,<sup>103</sup> or 'MPC'<sup>104</sup> sharding' arrangements, which are arrangements where the private key is split up into multiple parts ('shards') and each person holds one part of the key.<sup>105</sup> For example, many arrangements with custodial intermediaries involve '2 of 3 multisig' addresses, where there are three keys, and signatures from two keys are required to effect a transaction of

---

<sup>102</sup> For more detailed discussion, see Liu, 'Transfer Part 1' (n 3 above), 323-324.

<sup>103</sup> In this article, I cover multisig arrangements where the keys are held by different people, but multisig arrangements can also be used by one person (e.g. someone could have both sigs in a 2 of 2 multisig arrangement). In substance, the latter type of arrangement is functionally equivalent to a situation where one person has the private key to a single sig address and thus has exclusive positive and negative control. I will not be discussing this type of arrangement.

<sup>104</sup> Multi party computation.

<sup>105</sup> The Law Commission defines 'Sharding of keys' as "Splitting a single key into multiple pieces and copies of those pieces, such that some subset of the pieces can be recombined to recover and use the key for a signature and transaction": Law Commission, *Final report* (n 3 above), xiv.

the relevant digital asset.<sup>106</sup> In such cases, if a person (X) only has one key, he would not have positive control as he cannot unilaterally sign transactions on the blockchain in respect of the asset.<sup>107</sup> He would also not have negative control if another person (Y) has the other two keys, as he cannot prevent the other person from unilaterally signing transactions on the blockchain. However, X and Y collectively have positive and negative control as they have all three keys.

‘Limited control’ situations encompass any situation where there are programmed limits on a party’s ability to exercise control of a digital asset. Of course, such situations could arise when control is shared between multiple people, but they need not. For example, there can be escrow or collateral arrangements where digital assets are locked up in a smart contract for a period of time where no one has (immediate) control, and are only released to particular parties when certain conditions (such as payment, or production of documents, or default) are satisfied. In a collateral arrangement, the condition(s) in the smart contract could be that the digital assets (posted as collateral) are not in anyone’s control, but are (1) released to the lender in the event that the borrower defaults (such that the lender gains positive control of them), and (2) released to the borrower in the event that the loan is paid back (such that the borrower gains positive control of them).<sup>108</sup> In these arrangements, the programmed limits exist to ensure safety, prevent fraud, and reflect the intentions of the parties.

The position adopted by a legal regime in relation to what constitutes a sufficient ‘change of control’<sup>109</sup> depends on how one believes the balance between the relevant normative policy considerations should be struck.<sup>110</sup> In this regard, there is no ‘right answer’ per se as to how much weight to put on (e.g.) party autonomy, the encouragement of technological

---

<sup>106</sup> See text to nn 115-117 below.

<sup>107</sup> Given the two signature requirement for signing a transaction on the blockchain.

<sup>108</sup> See e.g. the NFTfi platform: ‘Borrow & lend on the leading NFT liquidity protocol’, *NFTfi* at <https://nftfi.com> (accessed 13<sup>th</sup> January 2025); see also Law Commission, *Consultation paper* (n 3 above), 18.78(1).

<sup>109</sup> To satisfy the transfer rule.

<sup>110</sup> See e.g. Liu, ‘Transfer Part 2’ (n 3 above), 251-254.

innovations, upholding market expectations and preventing unfair surprise, and mitigating against the risk of fraud. This is because opinions can legitimately differ as to which considerations to prioritise, especially in the context of different legal systems.

A legal system that prioritises the prevention of fraud over all other policy considerations may opt for a restrictive approach of only allowing title to be transferred where the transferee has all the keys to the address to which the digital asset is transferred. This would significantly limit the risk of ‘double sales’ as well as people’s ability to represent to third party creditors that they own the asset. Given that a sale can only happen with a full change of control, a seller of a digital asset will have completely transferred control of the digital asset to the buyer when title passes to the buyer. The person in control would be the buyer instead of the seller, meaning that the seller would not be able to represent to third parties that he owns the digital asset. As such, he would not be able to conduct a ‘double sale’ fraud.<sup>111</sup> Similarly, the fact that the seller does not retain control means he cannot credibly represent to third party creditors that he owns the asset.

The disadvantage of a requirement that the transferee obtain full control of a digital asset (in the sense of having all the keys to the address) is that it significantly limits party autonomy. Transfers of digital assets into custodial arrangements where there is a 2 of 3 multisig address and the transferee has 1 or 2 keys would not be sufficient to transfer title, and these arrangements are commonly used in the digital asset context because of certain benefits relating to safety and/or convenience.<sup>112</sup>

A legal system may view a ‘full control’ requirement to be too restrictive, and thus be more permissive. For example, it could allow a transfer of a property right in situations where the transferee has positive control (the ability to exercise the transactional functionalities and

---

<sup>111</sup> Unless he subsequently regains control of the digital asset.

<sup>112</sup> See e.g. ‘Introduction to the Best Multisig Wallets’, *Bitcoin Magazine* at <https://bitcoinmagazine.com/guides/best-multisig-wallets> (accessed 31 May 2024).

other benefits allowed by the asset) and negative control (the ability to prevent others from exercising such functionalities).<sup>113</sup> This would of course be the case where the transferee has all the keys to the address, but would also be the case if the transferee has two keys in a 2 of 3 multisig address. This is because him having two keys is sufficient to execute a blockchain instruction (positive control), and he can also prevent others from executing a blockchain instruction (negative control) given that a signature from one of his keys is required to meet the two signature requirement.<sup>114</sup>

A more relaxed approach in favour of party autonomy would be to allow the transfer of a property right where the transferee agrees to share control with someone else. This would be the case if for example he has some of the key(s), but has neither positive nor negative control (yet shares control with another person such that collectively, they have positive and negative control).

This would be the case where the transferee has one key in a 2 of 3 multisig address, where he agrees to share control with a custodian who has the other two keys. This is a common type of arrangement in the asset custody context, where the transferee (client) relies on the custodian's services to safeguard his assets and for administrative convenience. Specifically, under this arrangement, one key is held by the customer, and two keys are held by the custodian (one online, and one in cold storage<sup>115</sup>).<sup>116</sup> Assets can be transferred into the address, and if the customer wants to transfer them out of the address, he will sign with his one key, and the custodian will sign with one of its keys as well to satisfy the two signature requirement.

People sending tokens into this type of shared control address operate on the general assumption that there would be an effective transfer of title. Suppose A and B enter into a transaction for the sale of Bitcoin to B, and A transfers the Bitcoin into B's '2 of 3 multisig'

---

<sup>113</sup> See Section 8.2 below.

<sup>114</sup> Assuming no one else knows either or both of his two keys.

<sup>115</sup> Cold storage of a private key refers to storing the key in an offline environment.

<sup>116</sup> Bitcoin Magazine, 'Introduction to the Best Multisig Wallets' (n 112 above).

custodial wallet.<sup>117</sup> In this situation, A and B both expect that this would be sufficient to transfer title to B. This is because there has been a divestment of control by A (as transferor), and the Bitcoin goes into a different address that is managed on behalf of B. Although the transferee has no positive control,<sup>118</sup> the address is managed on B's behalf, and B has 'legal positive control' insofar as the custodian is contractually obliged to heed B's instructions.<sup>119</sup>

The DIFC, which is a pro-innovation jurisdiction, allows for title to be transferred in such situations.<sup>120</sup> The primary risk of such an approach is that since the person with whom control is shared can unilaterally misappropriate the asset (given that he has two keys and thus positive control), the transferee is (in this respect) less protected.

### 8.3 Types of control

After ascertaining which normative factors should be prioritised, one needs to decide what types of situations would be sufficient to transfer a property right. In other words, what types and degrees of change of control would be sufficient to transfer a property right?

Control arrangements in the digital asset context can be highly technical, so it is important to be clear on the various dimensions of control. Having these dimensions in mind means that (1) situations that initially seem different but are in fact similar enough can be treated alike, and (2) situations that initially seem similar but are fundamentally different in terms of the type and/or degree of control can be treated differently. This is important for two reasons. First, it helps legislators, law reform bodies and courts in ascertaining the precise range of situations where a property right can properly be said to have been transferred. Second, it

---

<sup>117</sup> In return for payment from B to A.

<sup>118</sup> 'Positive control' for the purpose of this chapter will be meant in the sense of *factual* positive control instead of *legal* positive control. The same applies in relation to 'negative control'. See Chapter 2, Section 3.3.1 para 1 for 'factual vs legal'.

<sup>119</sup> See also Chapter 2, Section 3.3.2 para 14 (in relation to legal positive control).

<sup>120</sup> DAL, Articles 12(1) and 10(3)(b).

minimises the risk of courts making false or irrelevant distinctions or analogies with existing situations that are sufficient (or insufficient) to transfer a property right when applying the relevant transfer rule, and thus helps the courts reason accurately.

It would be helpful to adopt a systematic approach when considering what situations should be sufficient to satisfy the ‘change of control’ requirement. In this regard, it is suggested that the change of control issue can be analysed through five dimensions:

1. (Factual) positive and/or negative control
2. Sole control
3. Amount of control lost by transferor or third party v amount of control gained by transferee
4. Conditions precedent and subsequent
5. Immediate control

### ***8.3.1 (Factual) positive versus negative control***

First, control can be analysed from the perspective of positive versus negative control (in a factual sense).<sup>121</sup> Positive control denotes the ability to exercise the transactional powers associated with the digital asset (such as transfer and/or voting, as the case may be). In turn, negative control denotes the ability to prevent others from exercising the transactional powers associated with the digital asset.<sup>122</sup>

One can have positive but not negative control and vice versa, and this is most evident in the multisig context. For example, if X has one key in a 1 of 3 multisig address, he has

---

<sup>121</sup> Instead of a legal sense (control via agreements entered into with others). See Chapter 2, Section 2.1.1 above for discussion of positive and negative control of digital assets.

<sup>122</sup> See Chapter 2, Section 2.1.1 paras 6-10 above.

positive control (as he can unilaterally effect transactions on the blockchain) but not negative control (as he cannot prevent the other two keyholders from effecting transactions on the blockchain, given one key is sufficient to effect a transaction). Conversely, if X has one key in a 2 of 2 multisig address, he has negative control (as he can prevent the other keyholder from effecting a transaction on the blockchain, given two keys are necessary to effect such a transaction), but he does not have positive control (given the two signature requirement means one key is insufficient to effect a transaction on the blockchain).

### ***8.3.2 Sole control***

The second dimension to be considered is whether the transferee has sole control (i.e. whether he is the only person who has control, or a certain type of control).<sup>123</sup> Thus, a person (X) would have sole positive and negative control if he has all three keys in a 2 of 3 multisig address, or two keys in such an address.<sup>124</sup>

He would not have sole positive control if he has one key in a 1 of 3 multisig address, because even though he has positive control in that he can unilaterally execute a blockchain transaction, so can the holders of the other two keys.

A person has sole negative control if he has (for example) two keys in a 2 of 3 multisig address, as he is the only person who can prevent a transaction from taking place. If the other

---

<sup>123</sup> I have used the terminology use of ‘sole’ because it avoids the potential ambiguity of the word ‘exclusive’. ‘Exclusive’ can be interpreted in two senses (see e.g. Hin Liu, ‘Title, control and possession in the digital asset world’ [2022] LMCLQ 597, 617): (1) exclusivity (the only person who can exercise control), and (2) excludability (the ability to exclude others from using the asset). The terminology of ‘sole’ refers to meaning (1).

<sup>124</sup> The other person (with only one key) cannot exercise positive control as he cannot unilaterally execute a blockchain transaction, given the two signature requirement. Nor can he exercise negative control as he cannot stop X from executing a blockchain transaction given X can unilaterally execute a transaction using his two keys.

key holder (Y) wants to execute a transaction and signs with his key, the original person (X) can prevent the transaction from being executed, by refusing to sign.<sup>125</sup>

A person would not have sole negative control if he has one key in a 4 of 4 multisig arrangement. The other key holders can also prevent an attempted transaction, by refusing to sign.

### ***8.3.3. Control lost by transferor v control gained by transferee***

Third, a change of control can be analysed from the perspective of how much control the transferor<sup>126</sup> loses, and how much control the transferee gains. These two elements need to be considered separately, because they are not always co-extensive.

It is often the case that (1) the transferor has sole positive and negative control, (2) he then loses all control when making the transfer to the transferee, and (3) the transferee gains sole positive and negative control. This would be the case where the transferor transfers a digital asset out of a single-sig address where he has the private key, into the transferee's address which is also a single-sig address where the transferee has the private key. In this sense the transferee gains the same degree of control that the transferor had immediately prior to the transfer.

However, there are many cases where how much control the transferor loses is different from how much control the transferee gains. An example would be where the transferor transfers a digital asset out of his single-sig address, into a '1 of 2 multisig' address where the transferee has one key and a custodian has the other key. The transferor loses both positive and negative control, but the transferee (1) only gains positive control (and not negative control),

---

<sup>125</sup> And of course one would have sole negative control if he has all the key(s) to an address.

<sup>126</sup> Or other person (with the consent or authority of the transferor), as the case may be. In this section I only discuss situations where the transferor has control (for the purposes of simplicity), but the analysis applies to where the person who has control is not the transferor.

and (2) such control is not sole positive control (given that the custodian also has positive control).

Nonetheless, the degree of control that the transferee can gain is contingent on how much control the transferor loses. If for example the transferor does not completely divest himself of his sole positive and negative control, the transferee cannot at the same time have sole positive and negative control. For example, if X executes a transfer of a digital asset from a single sig address into a 1 of 2 multisig address where X and Y each have one key, then both X and Y have positive control. The fact that X retains positive control means Y does not have negative control, and thus does not have sole positive and negative control.

#### ***8.3.4 Condition precedent and condition subsequent***

Fourth, one can consider whether there are any conditions precedent or conditions subsequent in relation to the transferor or transferee's control. These conditions appear in the smart contract context.<sup>127</sup>

In this context, a condition precedent is a programmed condition that needs to be fulfilled in advance before (positive and/or negative) control is obtained. This condition can be time-based, i.e. that the person will have control at a certain time. A time-based condition precedent to control ensures that, assuming the program runs as intended (i.e. in the absence of a bug or hack to the smart contract), the person will as a matter of certainty obtain control.

For example, if a smart contract is coded such that Y can exercise positive control of digital assets that are already in an existing address after 1<sup>st</sup> June 2025, then in the absence of

---

<sup>127</sup> Even in the Bitcoin context (where the scripting language is not Turing-complete), parties can use smart contracts, for example in the context of timelocked transactions (transactions that are valid only after a specified future date or block height): 'Bitcoin Smart Contracts and Apps: Do They Even Exist?' *Ledger* at <https://www.ledger.com/academy/bitcoin-smart-contracts-and-apps-do-they-even-exist> (accessed 22nd February 2024).

bugs or hacks to the smart contract address and/or underlying blockchain, it is guaranteed that Y can exercise control after 1<sup>st</sup> June 2025.

This kind of condition precedent where the condition is certain to happen contrasts with other condition precedents that are ‘act-based ’(based on an act performed by a person), or ‘event-based ’(based on an event). Act-based and event-based condition precedents generally involve conditions that may or may not happen.<sup>128</sup>

For example, if a smart contract is coded such that Y (a secured debtor) can exercise positive control of digital assets (the collateral for the loan) that are already in an existing address when the relevant loan is repaid, the condition precedent is the repayment of the loan.<sup>129</sup> This is something that may or may not happen, and so whether Y gains control is not guaranteed even if there is no bug or hack to the smart contract and/or underlying blockchain.

The same is the case in the context of escrow arrangements, under which Y gains control of the asset when the relevant conditions of the escrow arrangement (e.g. payment, the transfer of assets, the obtaining of licences or permits, and/or the presentation of conforming documents) are satisfied. These conditions may or may not be met as they are dependent on specific actions being performed.

A condition subsequent is the opposite of a condition precedent. In this context, it is a condition that, when met, causes a person who currently has control of a digital asset to lose control of it. This can again be time-based, act-based, or event-based. An example would be where someone currently has sole positive and negative control of a digital asset in a smart contract address, but the smart contract is programmed such that:

---

<sup>128</sup> Of course, some conditions precedent in this category are also (virtually) certain to happen – e.g. if the condition is that ‘the sun rises tomorrow’.

<sup>129</sup> E.g. in the context of the NFTfi platform mentioned at n 108 above.

- the asset will be automatically transferred out of the address after a certain date (time-based condition subsequent); or
- the asset will be automatically transferred out of the address if there is a default on a loan (event-based condition subsequent).

### ***8.3.5 Immediate control***

Fifth, one can consider whether a person has immediate control or not. This is essentially a temporal assessment of control. Immediate control refers to a situation where one can exercise control of the digital asset at the instant time with no delay. This excludes situations where one is currently unable to exercise control of the digital asset, but is programmed to be able to do so in the future after satisfying the relevant conditions set out in the code.

Linking this to the fourth dimension of control, ‘immediate control ’encompasses control subject to a condition subsequent, and control that is subject to no programmed conditions (whether precedent or subsequent). It does not encompass control subject to a condition precedent.

Overall, having an awareness of the analytical dimensions of control helps to determine much more precisely the range of situations that should be sufficient to transfer a property right.

### ***8.3.6 Consent-based conditions***

In addition to the five dimensions of control that have just been explored, one must also consider whether some of these dimensions of control need to be coupled with ‘consent-based ’ conditions involving the transferee. For example, one may consider that a party gaining a certain type of shared control is in itself insufficient for a property right to be transferred to that

party, but is sufficient<sup>130</sup> when the transferee consents to (e.g.) a control sharing arrangement with a third party. This is the position in the DAL.<sup>131</sup> One may also consider potential conditions in relation to who the relevant control is to be (consensually) shared with, (e.g. the transferor, or certain types of third parties).

### ***8.3.7 Avoiding false analogies or distinctions: practical examples***

As mentioned, the details of each shared or limited control arrangement can get highly technical, and if courts (or legislators or law reform bodies) are unclear on the different types and dimensions of control, this increases the risk of false analogies or distinctions. Awareness of the five dimensions of control explored above will help to mitigate this risk.

For example, suppose that one court (A) says X type and degree of change of control is sufficient to transfer a property right,<sup>132</sup> and another court (B) is faced with a situation involving Y type and degree of change of control. In this situation, court B needs to be sure that Y is ‘similar enough’ to X (in terms of change of control) to satisfy the relevant rule, in the case that (e.g.) X satisfies the rule in a borderline way, and court B is bound by court A’s decisions.

Of course, this depends on the rule/formulation that is adopted as well, and sometimes the rule provides a clear answer. However, the rule might be vague<sup>133</sup> and its wording does not identify the precise threshold required, so courts have to reason by analogy. It is in this situation that the analytical dimensions become especially relevant.

---

<sup>130</sup> Provided that the transferor has an intention to transfer title to the transferee.

<sup>131</sup> DAL, Article 10(3)(b) and Article 12(1).

<sup>132</sup> When coupled with an intention to transfer title to the transferee.

<sup>133</sup> E.g. if the Law Commission’s ‘change of control’ threshold (see text to nn 141-145 below) were to be adopted as the requirement (as applied to the context of transferring a property right).

An example would be as follows. Suppose one case (A) rules that a transfer into a 2 of 3 multisig address where the transferee has 2 keys (and a third party has one key) is sufficient to transfer a property right. If a judge in a subsequent case (B) is faced with a situation involving a transfer into a 1 of 2 multisig address where the transferee has one key (and a third party has the other key), would that be sufficient to transfer the transferor's property right?<sup>134</sup>

The difference here is that the transferee has positive control but no longer has negative control, and the question is whether this difference means that the transfer rule is not satisfied (such that the property right is not transferred). The judge in case B needs to be sensitive to the distinction between positive and negative control in order then to assess whether this difference in the present case (possibly when combined with other factors) is normatively significant enough for the purpose of the rule, such that the property right is not transferred. If the applicable rule is vague (such as 'sufficient change of control plus intention to transfer [the property right]'),<sup>135</sup> this becomes especially important as there is no clear guide as to where the threshold lies, and so both the normative balance and the analytical differences need to be carefully considered.

Another example would be as follows. Suppose that court decision A rules that a transfer into a smart contract address where the transferee has immediate positive control is sufficient to transfer a property right (despite someone else having immediate positive control as well). A judge in case B is now faced with a situation involving a transfer into a smart contract address where a third party has immediate positive control, and the transferee does not have immediate positive control but will do so after a certain amount of time (pursuant to a time-based condition precedent of the smart contract).<sup>136</sup>

---

<sup>134</sup> Assuming that the transferor has the intention to transfer his property right to the transferee.

<sup>135</sup> See text to nn 141-145 below.

<sup>136</sup> In the absence of bugs or hacks to the smart contract.

Again, as with the previous example, whether this is sufficient to transfer the property right would depend on whether it is analogous enough with the situation in decision A for the purpose of the relevant rule.<sup>137</sup> This again would require the court to be aware of the various dimensions of control, particularly conditions precedent.

A third example would be as follows. The situation is the same as the second example, but here the smart contract is programmed such that the transferee will obtain (immediate) positive control if he pays a sum into a particular address. Here, the transferee's positive control is conditional on his own conduct (under an action-based condition precedent), as opposed to subject to a time-based condition precedent. This difference is significant because the transferee may *never* have positive control even if the program works as intended. Unlike a time-based condition (which is certain to be satisfied), this action-based condition is dependent upon the transferee performing the action, which may or may not occur. The transferee may never make the payment.

A court may find that the degree of control that the transferee has is too low to satisfy the relevant rule, on the basis that the transferee may never have immediate positive control in the future under the smart contract even if the code works as intended, unlike with a time-based condition precedent (where the condition is certain to be satisfied). Yet, this requires the court to attend to the various dimensions of control, and being aware of the distinction between time-based and act-based conditions precedent would be highly useful.

Thus, it is crucial for courts to be clear on the different types and dimensions of control.

The Law Commission is recommending the creation of a panel of technical experts, lawyers, academics and judges to discuss factual and legal issues relating to 'control'.<sup>138</sup> It is suggested that this panel can help courts reach better decisions, and equip legislators with

---

<sup>137</sup> In the case that the rule is vague and does not provide a clear answer, for example if the Law Commission's 'change of control' threshold is adopted as the rule: see text to nn 141-145 below.

<sup>138</sup> Law Commission, *Final report* (n 3 above), 5.23 -5.28.

analytical tools that allow them to be more precise when debating which situations should be sufficient to transfer title (and thus a property right). The panel can consider these analytical dimensions when examining each type of shared control or limited control arrangement, especially new arrangements that may initially seem difficult to characterise.

#### **8.4 The linguistic formulation**

If one has (i) clarified the appropriate normative balance between the relevant considerations and (ii) ascertained what situations should be sufficient to transfer a property right to a digital asset, the final stage of the three-stage process is to formulate a rule that reflects the threshold in (ii) to a sufficient extent, while providing enough certainty and flexibility.

The considerations involved at this stage are:

- (1) reflecting the intended threshold as best as possible using the most appropriate form of wording;
- (2) providing enough flexibility in the rule in order to adapt to various situations;<sup>139</sup> and
- (3) providing enough certainty in the rule.

Of particular significance here are (2) and (3). In relation to (2), if there is insufficient flexibility in the rule, it would not cover all the situations it needs to, thereby running the risk of discouraging the use of blockchain technology in the future. In relation to (3), if there is insufficient certainty in the rule, parties would not know where they stand legally and this substantially increases the risk of stifling the use of certain shared and limited control arrangements.

---

<sup>139</sup> In particular, new technological arrangements and innovations.

These points do seem obvious but not all formulations that have been proposed satisfy both (2) (certainty) and (3) (flexibility). For example, the Law Commission in their 2023 Report suggested that title (and thus a property right) can be transferred where there is a ‘change of control’,<sup>140</sup> denoting a situation where the transferee is able “sufficiently” to exercise positive and negative control of the digital asset<sup>141</sup> and identify himself as the person with such abilities.<sup>142</sup> In trying to provide enough flexibility (i.e. satisfy factor (2)) and not stifle the (present and future) use of blockchain technology,<sup>143</sup> it is suggested that the Law Commission has produced a formulation that is too uncertain (i.e. does not satisfy factor (3)).

The formulation proposed is fundamentally circular, because the “sufficiently” threshold begs the very question of what type and degree of change of control is needed in order to transfer title (and thus a property right). It provides little substantive guidance to a judge as to how to decide a case that involves a partial change of control, and gives parties little certainty about what the substantive threshold for transferring title actually is. Although the Law Commission note that a body of jurisprudence can be developed by the courts in relation to what constitutes ‘control’,<sup>144</sup> the problem about circularity and uncertainty will remain until the position has been clarified by case law.

It is suggested that the rule adopted by the DIFC in the DAL is preferable in this regard as it provides a considerable degree of flexibility and is much more certain. Article 12 of the DAL provides that an *inter vivos* transfer of title is effective where there is a change of control to the transferee, coupled with an intention to transfer title to the transferee. In relation to

---

<sup>140</sup> Coupled with an intention requirement on the part of the transferor: Law Commission, *Final report* (n 3 above), 6.47.

<sup>141</sup> The ability to exclude others (negative control), and put the digital asset to the uses of which it is capable (positive control): Law Commission, *Final report* (n 3 above), 5.10.

<sup>142</sup> *ibid*, 5.10.

<sup>143</sup> *ibid*, 6.45.

<sup>144</sup> Law Commission, *Final report* (n 3 above), 6.45.

‘change of control’, the meaning of control is set out in Article 10, which is based on Principle 6 of the UNIDROIT Principles on Digital Assets and Private Law.<sup>145</sup>

Article 10(1) sets out a general ‘exclusivity’ threshold where one has control if he has (i) the ability to obtain substantially all the benefit of the digital asset (i.e. exercise the factual powers associated with the digital asset), (ii) the exclusive ability to prevent others from doing so, and (iii) the exclusive ability to transfer the above two abilities (i.e. (i) and (ii)) to another person.<sup>146</sup>

There are two ‘relaxations’ to this exclusivity threshold that are set out in Article 10(3):

*(a) the Digital Asset, or the relevant protocol or system, limits the use of, or is programmed to make changes to, the Digital Asset, including change or loss of control of the Digital Asset; or*

*(b) the person in control has agreed (expressly, by implication or by conduct) to sharing that ability with one or more other persons.<sup>147</sup>*

The first (Article 10(3)(a)) involves a ‘limited control’ situation. Specifically, if the transferee obtains control of a digital asset but his control is limited by how the protocol or smart contract is programmed, that is sufficient to transfer title.<sup>148</sup> Such limits could include a subsequent change or loss of control of the digital asset. The second (Article 10(3)(b)) involves a ‘consensual shared control’ situation, where if the transferee’s control of the digital asset is shared with other(s), and the transferee consents to such sharing of control, that would be sufficient to transfer title as well.<sup>149</sup>

---

<sup>145</sup> Principle 6 is adopted almost wholesale in Article 10 of the DAL. The only difference is that the relaxation in relation to consensual shared control in Article 10(3)(b) does not use the wording of ‘acquiesced’ in Principle 6(3)(b): see DIFC, *Consultation paper* (n 3 above), para 59 and footnote 34.

<sup>146</sup> DAL, Article 10(1)(a). One also needs to be able to identify oneself as having those abilities (10(1)(b)), but it is suggested that this is an evidential requirement. If one has such abilities, he would be able to identify himself as having them by (e.g.) signing a transaction on the blockchain.

<sup>147</sup> DAL, Article 10(3); DIFC, *Consultation paper* (n 3 above), para 69.

<sup>148</sup> DAL, Article 10(3)(a); DIFC, *Consultation paper* (n 3 above), paras 70-73.

<sup>149</sup> DAL, Article 10(3)(b).

In relation to factor (2) (flexibility), these relaxations do indeed provide for a high degree of flexibility, as they allow for transfer of title in many situations where the market expects the arrangement to give rise to a transfer of title. For example, in the ‘2 of 3 multisig custodial wallet’ arrangement discussed earlier,<sup>150</sup> title can be transferred to a wallet holder under such an arrangement despite him only holding one of the keys to the address (and thus not having positive or negative control). This is because he consensually shares control with the custodian, thus satisfying the ‘second relaxation’ in 10(3)(b).

As for factor (3) (certainty), these relaxations render the rule relatively certain, especially in comparison with the ‘sufficiently’ threshold proposed by the Law Commission. It is relatively easy to identify whether there are programmed limits to someone’s control or whether there has been consensual shared control. In the case of limited control, one just has to ascertain whether there are such programmed limits from the relevant code itself. In turn, in relation to consensual shared control, one merely has to ascertain whether there is an arrangement where the transferee shares control with another person (e.g. through a multisig or sharding arrangement), and determine whether the transferee has consented to such an arrangement. This stands in contrast with the Law Commission’s ‘sufficiently’ formulation where there is little substantive guidance as to how the rule is to be applied in concrete situations, resulting in an unacceptable amount of uncertainty.

Of course, whether a rule (actual or proposed) is certain or flexible *enough* is a subjective question upon which opinions may legitimately differ, and there may be critiques of any rule. Some may want a higher degree of certainty (to allow people in this relatively nascent market to be able to plan their affairs), while others may want a higher degree of flexibility (to accommodate for changing market expectations and fast technological innovations).

---

<sup>150</sup> See text to nn 115-117 above.

If one wants to raise issues or critiques when considering the merits of a particular rule, it is important to identify what any relevant critique relates to. Is it a critique that relates to there being too little certainty (vagueness), or too little flexibility (rigidity)? Or is it actually a critique about factor (1), i.e. how the linguistic formulation does not capture the intended threshold, and results in an overinclusive or underinclusive rule? Separating the three factors out helps to quickly identify the root of the critique or objection, and this is conducive to productive discussion about how the rule should be formulated and/or modified.<sup>151</sup>

### **8.5 The three-stage approach**

If a legal system or law reform body decides on having ‘change of control’ as the relevant requirement, it is suggested that they should take a three-stage approach when considering how best to formulate a ‘change of control’ rule, in line with the above discussion.<sup>152</sup> First, they should ascertain the ideal normative balance between the relevant policy considerations (such as party autonomy and the prevention of fraud). Second, they should ascertain what concrete situations would be sufficient to transfer title (with reference to the five dimensions of control discussed in Sections 8.3.1-8.3.5<sup>153</sup> above). Third, they should translate this concrete threshold into a rule/formulation that best encapsulates the threshold while providing enough certainty and flexibility.

---

<sup>151</sup> This minimises the risk of people talking past each other. For example, suppose X says that a formulation is unsatisfactory because it’s insufficiently certain, and Y believes there is no problem with the formulation because it reflects the intended threshold well enough. Y believes X is making a ‘factor 1’ critique, not seeing that it is actually a factor 2 critique, and thus does not answer his point. X and Y actually agree that there is no problem in relation to ‘factor 1’, but Y thinks X is disagreeing with him on that, but Y might not be present to the ‘certainty’ question (factor 2) independently of factor 1. Separating out the three factors helps to locate the critique much more quickly (by e.g. asking whether a particular critique is a factor 1 or a factor 2 critique). Having the three factors in mind also helps to surface additional issues about the rule and tackle them in advance.

<sup>152</sup> This mirrors the approach described in Liu, ‘Transfer Part 1’ (n 3 above), at 252.

<sup>153</sup> And any consent-based condition(s) (see Section 8.3.6 above).

## 9. On-chain transfer

Nonetheless, one may object to a ‘change of control’ formality requirement on the basis that it is not stringent enough. Another option would be to allow a property right to be transferred only in situations where there is an on-chain transfer (a ‘transfer operation that effects a state change’) plus an intention to transfer the property right. This was recommended by the Law Commission in their 2022 Consultation Paper<sup>154</sup> (in relation to the transfer of title, which by extension encompasses the transfer of a property right).

The rationale of such a requirement is based on the idea that there needs to be a sufficient degree of alignment between the blockchain entries and the location of title.<sup>155</sup> Under this rationale, maintaining a high degree of alignment via an on-chain transfer requirement would in turn increase the clarity and transparency of the ledger,<sup>156</sup> and thereby presumably limit the decouplings that substantially increase the risk of fraudulent conduct and defeated expectations.

However, it is suggested that an imposing an on-chain transfer requirement would be undesirable, for three reasons.

### 9.1 Party autonomy

First, imposing an ‘on-chain transfer’ requirement would be too restrictive of party autonomy. If off-chain transfers of control (e.g. via a USB stick, and under certain Layer 2 protocols) are insufficient to transfer title, this would be an unjustified restriction on party autonomy with no sufficiently important benefit. These methods can often be much cheaper than an on-chain

---

<sup>154</sup> Law Commission, *Consultation paper* (n 3 above), 13.141, 13.145, 13.22, and 13.32-35.

<sup>155</sup> *ibid*, 13.141: “any change in the state of the distributed ledger or structured record should generally correspond to a change in legal title to the relevant crypto-token”.

<sup>156</sup> *ibid*, 13.141.

transfer.<sup>157</sup> They can also be more convenient, as (for example) handing over a USB stick can be simpler than going through the process of executing an on-chain transfer. Also, as these off-chain methods do involve a change of control, the risk of fraud would not be substantially or disproportionately increased as compared to if an on-chain transfer requirement were to be imposed.<sup>158</sup>

## **9.2 On-chain transfer to self**

Second, if the ‘on-chain transfer’ requirement is interpreted literally, this would allow a property right to be transferred via an on-chain transfer to another address controlled by the transferor (provided that the transferor has an intention to transfer his property right to the transferee). This ‘on-chain transfer’ does not change control at all, and would decouple control and title completely, which creates opportunities for fraud (most notably, the transferor can fraudulently represent to a third party that he owns the asset, and cause harm to the transferee, subsequent purchaser(s), as well as creditors).

## **9.3 The ‘register’ justification**

The core justification for the ‘on-chain transfer’ requirement is based on the idea that the blockchain is analogous to a register (given that it is a ledger or database), and so there needs to be a high enough degree of ‘coupling’ between the ‘register entries’ and the location of

---

<sup>157</sup> On-chain transfers are often more expensive because of the gas fees (blockchain transaction fees) required.

<sup>158</sup> Having an on-chain transfer requirement (instead of a change of control requirement) would make it marginally more difficult for fraudulent assertion and denial to occur, but I have suggested that this marginal advantage does not justify the corresponding restriction on party autonomy: see Liu, ‘Transfer Part 1’ (n 3 above), 327 (fn98). The main point that applies to this thesis is that the (marginally) increased fraud risk does not justify the restriction on party autonomy. Also, the points in Sections 9.2 and 9.3 below further militate against introducing an on-chain transfer requirement.

title.<sup>159</sup> Otherwise, the blockchain would no longer be a reliable source for finding out who has title, and would not provide enough publicity, since not all transactions that involve the transfer of legal title would be publicised. Imposing an on-chain transfer requirement would therefore be necessary to protect third parties such as secured creditors.<sup>160</sup>

In other words, there must be a sufficiently high degree of coupling between ‘the information shown on the register’ and title, as opposed to coupling between control and title. However, it is suggested that the notion that the blockchain is a register rests on a false assumption. Ordinarily, a register contains the name of the person with the right, the property to which the right relates, and the right itself. For example, the Land Register contains (1) the name of the person with the right to or interest in the property, (2) the property that is the subject of the right or interest, and (3) the nature of the right or interest (e.g. the fee simple) that the person has over the property. The blockchain does not contain these elements. It is pseudonymous, and does not contain the name of the person who owns or controls the property. The information conveyed by the blockchain is which assets are in which (locked) spaces.<sup>161</sup>

This ‘register’ fallacy is attributable in part to the inferences that people make based on the premise that ‘the blockchain is a public database’ or ‘the blockchain is a public record of transactions’. These starting premises lead people to make the inference that ‘the blockchain is therefore a register’. However, this inference is fallacious as it is missing the necessary premise of ‘the record shows the name of the interest holder, the asset, and the interest’.

---

<sup>159</sup> This is based on my conversations with industry participants and academics. See also e.g. Law Commission, *Consultation paper* (n 3 above), 13.141: “any change in the state of the distributed ledger or structured record should generally correspond to a change in legal title to the relevant crypto-token”. This was one of the reasons why it recommended an on-chain transfer requirement in the Consultation Paper.

<sup>160</sup> In relation to purchasers, the Law Commission has recommended a general bona fide purchaser rule that applies to all crypto-assets (see n 96 above), and many academics and market participants agree with this stance. If this is adopted, a ‘change of control’ rule would perform the function of protecting good faith purchasers that obtain control of an asset from an existing address (as they would obtain title).

<sup>161</sup> Locked spaces ie public addresses.

‘Correspondence’ or ‘coupling’ between the information shown and legal title<sup>162</sup> is required to the extent that it is necessary to protect third party reliance on the information shown on the register. When a person relies on some information or data from the external world, that data is causing him to form a belief as to a state of affairs, which he subsequently acts on. In the case of the Land Register, people use the register entries to form beliefs about who has legal title, and reasonably expect the entries to be accurate, given that it is a government-run national register. They act on such beliefs by purchasing property or taking an interest in it, and so there is a need to protect such reliance by coupling the records with legal title.<sup>163</sup> Indeed, the Land Register is expressly designed to encourage reliance on the register entries to find out who has legal title.<sup>164</sup>

Indeed, if the location of title were to be decoupled from the register entries, then purchasers and creditors would suffer. A purchaser may not gain good title when he relies on the register entry showing that the vendor is ‘owner’ of the property (especially in the absence of a wide bona fide purchaser rule), and a creditor would have less collateral<sup>165</sup> to enforce against if the debtor does not own the property (contrary to what is shown on the register). Thus with the Land Register, there is a need to protect third party reliance through imposing a formality rule that ensures the coupling of title with the register entries.

It is important to note that ‘reliance’ in relation to particular information/data<sup>166</sup> consists of two stages: the ‘external input’ stage and the ‘verification’ stage. First, there is an ‘external input’ (data one observes from the world, such as a register entry) which causes a person to infer or assume that a particular conclusion is true. Second, this reduces (or eliminates) the

---

<sup>162</sup> In the Land Register context this is referred to as the ‘mirror principle’.

<sup>163</sup> Section 58 of the Land Registration Act 2002 (“LRA”) provides a one-to-one correspondence between the records and legal title.

<sup>164</sup> As evidenced by LRA s58.

<sup>165</sup> Or no collateral, if the only asset that is the intended subject of the security interest is the land in question.

<sup>166</sup> I am referring to reliance on factual information/representations, as opposed to reliance on *promises*, in (for example) the estoppel context.

effort he expends in verifying whether the conclusion is true. Where there is a high degree of (reasonable) reliance in relation to the two stages, this militates in favour of a high degree of ‘correspondence’ between the information shown and legal title.

On the other hand, if the relevant information provided (or quality of the ‘information signal’) is insufficient, a reasonable person might not assume (even provisionally) that a conclusion (in this case that the person shown on the records has legal title) is true, and as such, he would independently verify whether the conclusion is true. In this case, there is no reliance that the law ought to protect through providing a high degree of ‘correspondence’ between the ‘information signal’ and the relevant conclusion, which in this context would be that the person has legal title. This is because the downside of maintaining a high (or complete) degree of correspondence between the records and title through imposing the requisite formality rule is that it stifles party autonomy. Party autonomy should be respected unless there is an overriding reason (primarily in relation to the protection of third parties) that justifies such a formality requirement.

In relation to physical goods, there is a lower degree of ‘reliance’ on a person’s possession of an asset in inferring that he has title, as compared to the reliance that people place on the Land Register records in indicating the location of legal title. This is because although we make the general assumption that if one possesses a physical asset he has title to it, we also know that there are many arrangements in respect of goods that involve the person possessing the good not being the owner (such as hire or hire purchase arrangements),<sup>167</sup> i.e. where title is decoupled from control. Thus, even if the external input (X having control of a physical asset) leads a person to make the general assumption that a conclusion (X having title to the asset) is true, that does not replace his independent verification and judgement as much as in the case

---

<sup>167</sup> In hire purchase arrangements, the hirer does not obtain title until he exercises the option to purchase the asset.

of the Land Register. Often, he would make his own inquiries to confirm whether the initial assumption is true,<sup>168</sup> resulting in a lower degree of ‘reliance’.

In the blockchain context, there is an even lower degree of reliance on the ‘information’ shown on the blockchain in inferring the location of title, since third parties would not know who owns or controls which assets: they are just given the virtual location of each asset.<sup>169</sup> Thus, the initial ‘external input’ given by the blockchain does not lead the reasonable person to assume that a particular identified person has title (in contrast with the physical asset context).<sup>170</sup> It merely leads the reasonable person to assume that the person who has control of the assets in the address has title. As such, if he wants to find out who has title to certain digital assets, he would need to independently establish that a person<sup>171</sup> has control of the assets in the relevant address, to engage the general assumption that such person has title to them. To prove control (ie to mirror the ‘physical possession’ threshold for chattels), the person purporting to have control of the digital assets can sign a message/signature using his private key, which proves that he has such control.<sup>172</sup> As such, it would be reasonable to require third parties to first ensure that the person they are transacting with has control.<sup>173</sup> Even at this point however, what is engaged is merely the *general* assumption that the person has title by virtue of his control, and further independent inquiries need to be made to verify whether this assumption is true.<sup>174</sup> These inquiries cannot be satisfied by looking at the blockchain.

---

<sup>168</sup> For example in the context of high value goods like rare paintings.

<sup>169</sup> Unlike the Land Register, there is limited information provided by the blockchain.

<sup>170</sup> Most people view and search blockchain entries through block explorers, instead of downloading a copy of the blockchain. Block explorers are websites that “enable...you to search for real-time and historical information about a blockchain”: see ‘What is a Block Explorer? BTC Block Explorers, etc. | Gemini’, *Gemini* at <https://www.gemini.com/cryptopedia/what-is-a-block-explorerer-btc-bch-eth-ltc#section-the-block-explorer-a-window-into-the-blockchain> (accessed 2 April 2023).

<sup>171</sup> Or multiple people, in the case of a multisig address.

<sup>172</sup> There are other ways for a person to prove control, e.g. by logging into one’s digital asset wallet in someone’s physical presence.

<sup>173</sup> Of course, if there is a general BFP rule and you are purchasing the good, you would not need to do this (since if you purchase the asset in good faith without notice, you would obtain clean title).

<sup>174</sup> In practice, people generally do not go through this verification process. For example, people just purchase a digital asset as long as they know the asset can be transferred into their address. They do not care who the seller is. In such a situation, there is simply no reliance on any information given on the blockchain.

Thus, in the blockchain context, there is no ‘reasonable reliance’ that ought to be protected by imposing the degree of coupling demanded by an on-chain transfer requirement. The on-chain transfer requirement rests on the ‘register’ analogy, and such an analogy rests on the idea of protecting parties who reasonably rely on information provided by the ‘register’.<sup>175</sup> In this regard, the blockchain cannot serve the purpose that the Land Register is designed to serve (encouraging reliance on the information provided to ascertain who has legal title),<sup>176</sup> because it simply does not provide the necessary information.<sup>177</sup>

#### 9.4 Protection of secured creditors?

Nonetheless, despite the three reasons mentioned above, there is a concern that if a property right can be transferred off-chain, this would provide insufficient protection for secured creditors. This is on the basis that they would not be able to tell when the debtor has transferred its property right<sup>178</sup> to the asset<sup>179</sup> (thus giving the creditor fewer assets to enforce against), given that there is no positive publicity where an off-chain transfer happens.<sup>180</sup> This argument

---

<sup>175</sup> An ‘on-chain transfer’ requirement goes further than the analogy with delivery of a physical asset. An on-chain transfer provides publicity of a transaction, but delivery merely gives you the *potential* to (positively) publicise your control (and such publicity is not an automatic consequence).

<sup>176</sup> Also, the Land Register is designed to be a *state-backed* guarantee of title.

<sup>177</sup> One may nonetheless argue that people rely on block explorer ‘tags’ in determining who has title to a digital asset. In many block explorers (such as Etherscan), one can ‘tag’ their name to an address by (for example) signing a signature with the private key to that address, and this tag is shown on the block explorer. People may thus rely on these tags in making the inference that the ‘tagger’ has title to the digital assets in his address.

However, it is suggested that it is unreasonable to rely purely on block explorer ‘tags’. First, the tag may be inaccurate because “it may be later reported that a user was falsely claiming to own a specific address”: see Public Name Tags, Labels & Public Notes, *Etherscan* at <https://info.etherscan.com/public-name-tags-labels-public-notes/> (accessed 31 March 2023). Second, even if the ‘tagger’ had control of the address at the time the address was tagged, the tags are not dynamically updated. The tagger could have changed control of the address off-chain, such that he has no control anymore. Third, these block explorer ‘tags’ are not information *on the blockchain*: they are information given by a separate company or organisation.

In any event, if there is a general BFP rule (as the Law Commission recommends), people who rely on block explorer tags when purchasing a digital asset are still protected, since they would obtain clean title if they are a bona fide purchaser for value without notice.

<sup>178</sup> And thus title: see the two assumptions made at n 5 above.

<sup>179</sup> E.g. where there is a USB change of control.

<sup>180</sup> This is similar to the argument made in *Private Equity Insurance Group SIA v Swedbank AS* (C-156/15) [2017] EU:C:2016:851; [2017] 1 WLR 1602; [2017] 1 BCLC 207 concerning the risk that a secured creditor may withdraw the relevant collateral before enforcement. This is what Gullifer refers to as “fraudulent removal

would therefore suggest that an ‘on-chain transfer’ requirement is necessary to provide enough publicity. However, it is suggested that in such situations, secured creditors should be protecting themselves. Creditors can bargain for more protection, for example in the form of a transfer of the collateral into a multisig address over which the creditor has negative control, or into an address over which the creditor has sole positive and negative control.<sup>181</sup> They may also simply adjust the terms of their arrangement to account for the risk of the debtor transferring his property right to the asset off-chain.

## 9.5 Summary

It is clear that having an on-chain transfer requirement for transferring a property right to a digital asset suffers from various problems, and is an inferior alternative to imposing a ‘change of control’ requirement. Thus, it should not be adopted.

## 10. Conclusion

This chapter has argued that a ‘change of control’ (coupled with an intention to transfer one’s property right) should be the requirement for transferring a property right to a digital asset. The risks of fraudulent conduct (in the form of fraudulent assertion, fraudulent denial, and double sales), and the relative ease of transferring control of a digital asset, mean that an ‘agreement’ rule analogous to the sale of goods cannot be applied in the digital asset context. Similarly, having a ‘deed’ requirement would be disastrous, most crucially because it allows for the free

---

risk” (see Roy Goode and Louise Gullifer, *Goode and Gullifer on Legal Problems of Credit and Security*, (6th ed, Sweet & Maxwell 2017), 4-22), 6-49. On the other hand, if there is an on-chain transfer requirement, there will be positive publicity of transactions that involve the transfer of legal title.

<sup>181</sup> This is analogous to Louise Gullifer’s critique of *Swedbank* (see Goode and Gullifer (n 180 above), 6-49), where she suggests that “fraudulent removal risk” by the collateral-provider is a risk that the parties themselves should manage: it is the collateral-taker who should bargain for more protection.

decoupling between control and title (giving rise to the risk of double sales), and actively prevents people from transferring title even where there *has* been an on-chain transfer under which the transferee obtains control.

Such disadvantages can be addressed using a ‘change of control’ requirement, which directly defines the threshold in terms of the very condition that increases coupling between control and title, and significantly reduces the instances of fraud. A change of control happens relatively quickly (i.e. via executing an on-chain transfer or an off-chain change of control), and is a requirement that is relatively easy for people to satisfy. Also, contrary to the Law Commission’s 2022 Report, requiring an on-chain transfer would be undesirable.

Deciding on the appropriate ‘change of control’ rule to adopt, especially when considering digital asset arrangements that involve shared control and limited control, is no easy task and does not yield one definitive ‘right answer’. Opinions can legitimately differ about (1) the appropriate balance between the normative policy factors, (2) the concrete situations that should be considered sufficient for a property right to be transferred, and (3) how to produce a rule or formulation that reflects the intended threshold well enough, and provides enough certainty and flexibility.

A three-step structure has been proposed<sup>182</sup> for deciding what the ‘change of control’ rule should be, in a way that gives effect to the above factors. This structure provides a framework that can be applied by a legislature or court (or law reform body) that is considering the relevant rule to adopt, and can assist a court that is faced with specific issues on transfers of property rights, especially in the shared or limited control contexts.

---

<sup>182</sup> In Section 8.5 above.

## **Chapter 4: Protection against interference**

### **1. Introduction**

The previous two chapters explored the circumstances under which a property right in respect of a digital asset ought to be acquired and transferred. This chapter explores the question of how a property right in respect of a digital asset should be protected against interferences. Specifically, under what circumstances can and should a person with a property right be able to successfully sue a defendant who interferes with his ability to exercise the transactional power(s) associated with the digital asset? In other words, what is the strength of a property right in respect of a digital asset, against third parties generally?

This ‘protection’ issue is crucial to explore because it informs the scope of protection offered to a holder of a property right in a digital asset, and thus the extent to which the (present and future) use of his digital asset is protected by the law. This chapter extends the earlier discussion in Chapter 1 about property rights in respect of digital assets.

It is also a question of immediate relevance because as the law currently stands, there is an obvious gap in the level of legal protection offered to holders of digital assets. Most crucially, several ‘core cases’ of interference with a digital asset (such as intentionally<sup>1</sup> burning and freezing a digital asset) do not necessarily yield any remedy under the current law. Also, there is no remedy in many situations where someone denies the claimant the ability to access his digital asset or exercise its functionalities – a position which one may think provides insufficient protection to property right holders. Indeed, although there is clearly a gap in respect of the ‘core cases’, the size of the ‘gap’ in protection in relation to digital assets is

---

<sup>1</sup> Where the defendant (1) knows that someone else has a (better) property right to the digital asset in question (including property right of any strength, if the defendant does not have any property right), and (2) does not believe that the person with the property right has consented to the relevant action(s): see Section 4.1.2 below.

debatable, as it depends on what one believes should be the extent to which a person's use of their digital asset ought to be protected.

Limitations of space preclude a detailed discussion of every issue in relation to protection,<sup>2</sup> but this chapter will discuss the 'gap' in protection and potential ways to fill such a gap. It will also set out the general approach and *prima facie* threshold<sup>3</sup> in relation to what the scope of protection in respect of a digital asset should be, as well as the best legal mechanism to achieve such protection.

Linking this back to the discussion of 'aim, substance and technique',<sup>4</sup> the *prima facie* threshold of protection corresponds with the 'substance' level' and the legal mechanism to achieve such protection corresponds with the 'technique' level. The general approach adopted in this chapter is not to apply rules developed in relation to physical assets (just because they involve property rights) – but rather to carefully consider the balance to be struck between holders of digital assets and other people. The aim in both the physical and digital asset contexts is the same (to provide the most appropriate level of protection), but (as will be seen in this chapter) the substance of the proposed protection regime in respect of digital assets, as well as the legal techniques used, are very different to the regime in respect of physical assets.

## **1.1 Structure of chapter**

This chapter will be structured as follows. First, I will explore the gap in protection in respect of digital assets, by exploring the 'core cases' where there should be liability, and how the current law does not provide protection in many of these 'core cases'. I will also explore the question of how big this gap in protection could potentially be.

---

<sup>2</sup> E.g. in relation to defences, the precise situations that do and do not constitute an impairment of use.

<sup>3</sup> Excluding defences.

<sup>4</sup> Introduction, Section 2.3 above.

I will then explore the potential solutions in relation to how the gap is to be filled. Two solutions will be explored: (1) extending the chattel torts, and (2) formulating a new regime that involves an interference and a ‘recovery of control’ remedy. It is suggested that the first option is unsatisfactory, and the second option points the way forward.

Under the second option, the impairment tort would allow someone with a property right to a digital asset to sue a defendant who intentionally or recklessly impairs the use of his digital asset.<sup>5</sup> In turn, the ‘recovery of control’ remedy would allow someone with a property right to a digital asset who does not have control of a digital asset to recover control of it.<sup>6</sup>

## **2. The gap in protection**

As the law currently stands, there is insufficient protection offered to someone who has a property right in a digital asset.<sup>7</sup> There are insufficient remedies for someone whose ability to use their digital asset has been interfered with, and this creates a ‘gap’ in protection.

The ‘gap’ clearly exists in several obvious ‘core situations’ where someone’s digital asset has been interfered with, in the sense that the number of functionalities they can exercise in relation to a digital asset using their private key has been diminished. The gap exists in many (but not all) of these ‘core situations’.

### **2.1 The ‘core situations’ of interference**

---

<sup>5</sup> This is a simplified overview – the elements of the impairment tort will be explored in more detail in Section 4.1 below.

<sup>6</sup> This is a simplified overview – the elements of the ‘recovery of control’ remedy will be explored in more detail in Section 4.2 below.

<sup>7</sup> Or more accurately, a person who would have a property right to a digital asset under the rules explored in Chapters 2 and 3.

In this regard, what are the ‘core situations’ where the claimant’s ability to exercise his transactional powers has been interfered with by a defendant?

It is suggested that misappropriating the asset from the relevant address over which the claimant has control (by changing control of the digital asset to an address controlled by the defendant, and depriving the claimant of control) is one such ‘core case’. The claimant no longer has control as a result of the defendant’s conduct, and thus no longer has the ability to exercise the transactional power(s) associated with the digital asset.

‘Burning’ and ‘freezing’ a digital asset would also be ‘core cases’. Burning a digital asset involves (1) destroying it outright, or (2) transferring it into an address where there is no private key (a ‘burn address’). In relation to (2), although the digital asset technically ‘remains’ in the burn address, it is rendered functionally obsolete, because no one can have control of the digital asset anymore, and no one can enter any transactions in respect of the digital asset.

Freezing<sup>8</sup> involves disabling someone from being able to enter blockchain transactions in respect of the digital asset (or at a minimum, disabling someone from transferring the digital asset to another address). This contrasts with burning, where the digital asset does not remain in the address but is either sent to the ‘burn address’ or destroyed. Also, when a digital asset is frozen, it can often be ‘unfrozen’ with the effect that the ability to enter blockchain transactions in respect of the digital asset would be restored.

I will be adopting a relatively narrow meaning of ‘freezing’, which only encompasses restrictions on transactional abilities at the blockchain or code level, meaning that the property right holder is restricted or disabled from entering into blockchain transactions even when he has the private key. This contrasts with the wider meaning of ‘freezing’, which involves (e.g.) an exchange that has full control of (and most often the property right to)<sup>9</sup> a digital asset and

---

<sup>8</sup> Which has also been called ‘locking’.

<sup>9</sup> See e.g. Hin Liu, Louise Gullifer and Henry Chong, ‘Client-Intermediary Relations in the Crypto-Asset World’ in Paul Davies and Tan Cheng-Han (eds), *Intermediaries in Commercial Law* (Hart Publishing, 2022), 213, 214. The exchange is most likely to be holding the property right to the digital asset on trust for the client.

restricts its client from being able to direct it to transfer the digital asset to another address or enter trades on the platform. In the latter case, there is no restriction imposed at the blockchain or code level.

## **2.2 Liability for intentional misappropriation, burning or freezing**

Where someone misappropriates, burns, or freezes a digital asset, this should clearly give rise to liability (subject to defences) when he does so intentionally with the knowledge that he has no property right to it (or that he does not have the best property right to it), has no belief that he has the consent of the property right holder(s) to perform the relevant action(s), and the claimant knows his private key.<sup>10</sup>

Given that property rights in digital assets are intended to protect people's ability to use their digital assets,<sup>11</sup> it becomes abundantly clear why these situations should give rise to liability.

### ***2.2.1 The conduct element***

When a digital asset is misappropriated or burnt from an address controlled by the property right holder,<sup>12</sup> the property right holder's use of that digital asset is totally impaired. In the case of misappropriation and burning, he has no control over the digital asset as he cannot exercise any transactional functionalities in respect of it.

Similarly, when such a digital asset is frozen, the property right holder cannot execute any transactions on the blockchain in respect of the digital asset (or at a minimum, cannot

---

<sup>10</sup> Unless otherwise specified in this chapter, it will be assumed that the claimant knows his private key when the defendant performs the relevant action(s) or otherwise impairs the use of the claimant's digital asset(s).

<sup>11</sup> See Chapter 1, Section 6.3.1 above.

<sup>12</sup> I.e. an address where he knows the private key.

execute a transaction to transfer the asset to another address).<sup>13</sup> At a minimum, this is a severe impairment of use, especially since the main use of many digital assets is the ability to transfer it to another address.<sup>14</sup>

Given that the core aim of conferring a property right in respect of a digital asset is to protect someone's use of a digital asset, it is clear why intentional burning and freezing deserve protection. These actions involve a total or severe impairment of use, and should give rise to prima facie liability, provided that the mental requirement is not overly harsh on the defendant.

### ***2.2.2 The mental element***

At this point one may argue that totally (or severely) depriving a property right holder from the use of their asset should not give rise to liability *per se*, but only when the defendant's mental state is egregious enough.

It is suggested that the actions of misappropriation, burning, and freezing should clearly give rise to liability when the defendant intends to cause this outcome while (1) knowing that someone else has a property right to the digital asset in question, and (2) not believing that the person with the property right has consented to the relevant action(s). This would be a clear case of liability because the defendant's mental state is the most egregious.<sup>15</sup> There is no 'mitigating factor' such as a lack of awareness that someone else has a property right, or a lack of foresight about the intended effect of his actions.

---

<sup>13</sup> One can still execute blockchain transactions to (for example) vote, bid, or claim an airdrop, if they exist in respect of the asset.

<sup>14</sup> For example, the only transactional functionality available in respect of Bitcoin is the ability to transfer it to another address.

<sup>15</sup> See e.g. Christina McAlhane and Natalie Wortley, *Criminal Law – The Fundamentals* (4<sup>th</sup> ed, Sweet & Maxwell, 2016) 3-005 – “Intention is perceived as being the most serious form of mens rea, presumably because it involves a defendant *deliberately* choosing to act in such a way as to bring about a certain consequence. A defendant who acts with intention is considered to be more culpable than someone who merely foresees the consequence (recklessness) or acts carelessly (negligence)” (emphasis added).

## 2.3 The current law leaves gaps in protection

As the current law stands, there is no remedy available even in some of these ‘core case’ situations. A constructive trust is available where a digital asset has been misappropriated,<sup>16</sup> but in respect of intentional burning and freezing, the claimant remains unprotected in many situations.

In relation to the chattel torts (conversion, trespass and reversionary injury), these torts only apply to chattels.<sup>17</sup> Thus, they do not offer a remedy when there is no ‘anchor’ physical asset that has been interfered with, such as a USB device that stores the private key, or a piece of paper where the private key is written down. In the case where a digital asset is burnt or frozen without any interference or contact with a physical asset owned by the claimant (e.g. where the defendant knows the claimant’s private key and sends the asset into a burn address), there is no remedy under the chattel torts.<sup>18</sup>

The economic torts also do not provide sufficient protection in relation to burning or freezing a digital asset.

First, inducing breach of contract would not be of assistance outside the contractual context since (*inter alia*) a prior contract and knowledge of such contract is required.<sup>19</sup> The act of intentional freezing or burning must amount to a breach of contract (and this is not the case where there is no prior contract), and even if this is the case, the defendant must realise that the intentional burning or freezing of the claimant’s digital asset amounts to a breach of that contract (which might not be the case).<sup>20</sup>

---

<sup>16</sup> See e.g. *Bybit Fintech Ltd v Ho Kai Xin* [2023] SGHC 199; citing *Westdeutsche Landesbank Girozentrale v Islington London Borough Council* [1996] 1 AC 669, 716.

<sup>17</sup> And electronic trade documents: see discussion in Hin Liu, ‘Interference torts in the digital asset world’ (2025) 84 CLJ (forthcoming); Electronic Trade Documents Act 2023, s.3.

<sup>18</sup> Unless they are an electronic trade document (see Liu, ‘Interference torts’ (n 17 above)), which the vast majority of digital assets are not.

<sup>19</sup> *OBG Ltd v Allan* [2007] UKHL 21, [2008] 1 AC 1, [39]; and see generally [39]-[44] for the requirements of the tort.

<sup>20</sup> E.g. the defendant has no knowledge of the contract or has no knowledge about its terms.

Second, in relation to the ‘causing loss by unlawful means’ tort, the defendant (D) needs to (1) use unlawful means (in the sense of a civil wrong) against a third party X that affects X’s liberty to deal with the claimant (C),<sup>21</sup> and (2) intend to cause loss to C.<sup>22</sup> Thus, even if D spots a smart contract loophole and freezes or burns C’s digital assets by directly interacting with the blockchain, that does not constitute unlawful means for the purpose of the unlawful means tort. There is no civil wrong that has been committed.

Third, deceit requires the defendant to make a representation and for the claimant to rely on it,<sup>23</sup> which would not apply in cases where the interference does not require the cooperation of the claimant, and in cases where the defendant makes no representation to the claimant. It therefore does not cover many situations involving intentional burning and freezing, e.g. where the defendant spots a bug in a smart contract that allows him to send the claimant’s digital assets into a burn address without the claimant’s knowledge, and intentionally exploits that bug.<sup>24</sup>

Fourth, other economic torts such as conspiracy or intimidation offer limited assistance. The conspiracy torts (lawful and unlawful means conspiracy) require some sort of combination, and therefore provide no protection in cases where the defendant acts alone in intentionally burning or freezing the claimant’s digital asset.<sup>25</sup> In turn, the tort of intimidation requires a threat,<sup>26</sup> which in most cases of freezing and burning, does not exist since the relevant actions are executed via a computer without any communication with another person.

---

<sup>21</sup> *OBG* (n 19 above), [29] and [51]; *Secretary of State for Health v Servier Laboratories Ltd* [2020] Ch 717; James Goudkamp and Donal Nolan, *Winfield and Jolowicz on Tort* (20<sup>th</sup> ed, Sweet & Maxwell 2020), 19-023.

<sup>22</sup> *OBG* (n 19 above), [62], and [164]-[167].

<sup>23</sup> See Michael A Jones, Anthony M Dugdale, Mark Simpson, *Clerk and Lindsell on Torts* (24<sup>th</sup> edition, Sweet & Maxwell 2023), 17-05 and 17-35.

<sup>24</sup> Without any mistaken belief that he has a property right to the asset or that the claimant has consented to the exploitation of the bug.

<sup>25</sup> Conspiracy requires concerted action between two or more people: Goudkamp and Nolan (n 21 above), 19-039 and 19-041.

<sup>26</sup> The tort of intimidation requires a “threat by the defendant to do something unlawful or ‘illegitimate’”: *Berezovsky v Abramovich* [2011] EWCA Civ 153, [2011] 1 WLR 2290, [5].

Unjust enrichment is also of limited assistance, because neither freezing nor burning involve an enrichment to the defendant. In any event, there are issues with establishing the unjust factor.<sup>27</sup>

Other causes of action in the intellectual property space (e.g. copyright infringement) and the data protection space (e.g. misuse of private information)<sup>28</sup> also do not assist in most cases of freezing and burning. When a digital asset is burnt by the defendant executing a blockchain instruction to send the asset into a burn address, there is usually no intellectual property right that is being infringed – for example there is no copying or reproduction that constitutes a copyright infringement.<sup>29</sup> Also, in terms of misuse of private information and breach of confidence, these mainly cover the unauthorised use<sup>30</sup> and disclosure<sup>31</sup> of confidential or private information.<sup>32</sup> Where a token is burned or frozen, there is usually no use or disclosure of confidential or private information. Most situations where a token is burned or frozen do not involve knowledge of the tokenholder’s private key.<sup>33</sup>

There is also a further issue relating to the characterisation of damage to a digital asset in the negligence context. If one is recovering for negligently caused *property damage*, the rules on recovery are much more pro-claimant than recovery of negligently caused *economic loss*. Currently, the case law assumes that ‘property’ means tangible property,<sup>34</sup> and so property

---

<sup>27</sup> There is no mistake by the claimant, no failure of consideration, and no duress or undue influence. The closest unjust factor is the possible unjust factor of ‘ignorance’ (also formulated as ‘lack of consent’, or ‘want of authority’, or ‘powerlessness’), but there is “some doubt” as to “whether the law of unjust enrichment recognises any of these unjust factors”: Rory Gregson, ‘Is subrogation a remedy for unjust enrichment?’ (2020) 136 LQR 481, 488. See also William Swadling, ‘Ignorance and Unjust Enrichment: The Problem of Title’ (2008) 28 OJLS 627; William Swadling, ‘Policy Arguments for Proprietary Restitution’ (2008) 28 LS 506; Tatiana Cutts, ‘Modern Money Had and Received’ (2018) 38 OJLS 1 at 9.

<sup>28</sup> See e.g. *Campbell v Mirror Group Newspapers* [2004] UKHL 22, 2 AC 457.

<sup>29</sup> And even if a token is linked to an intellectual property right (e.g. in the case of some NFTs), burning the NFT does not constitute an *infringement* of the relevant intellectual property right.

<sup>30</sup> See e.g. *CC Kent Police v Taylor* [2022] EWHC 737; *Prince Jefri Bolkiah v KPMG* [1998] UKHL 52, [1999] 2 AC 222.

<sup>31</sup> See e.g. *Tchenguiz v Imerman* [2010] EWCA Civ 908, [2011] 2 WLR 592, [69] and [72].

<sup>32</sup> See generally Jones et al (n 23 above), Ch 25.

<sup>33</sup> For example, where a global freeze permission is exercised, where a smart contract burn function is called.

<sup>34</sup> See e.g. *Murphy v Brentwood DC* [1991] UKHL 2, [1991] 1 AC 398; Jones et al (n 23 above), 1-51; Goudkamp and Nolan (n 21 above), 7-015.

damage would not at the moment seem to cover destruction of a digital asset. A claimant needs to satisfy the (much more stringent) rules in respect of economic loss, which require an assumption of responsibility and/or reliance.<sup>35</sup>

From this analysis it is clear that the law's protection against the intentional burning and freezing of a digital asset is deficient. There are serious gaps in protection that need to be filled.

## 2.4 How big is the gap?

It is clear that there is a gap in protection in respect of digital assets, and this raises the question of how big such a gap is. The answer to this question depends on one's stance to how much one wants to protect a property right holder's ability to use his digital asset. The more the law protects the property right holder's ability to use his digital asset, the more onerous the corresponding duties are on third parties not to interfere with such an ability, and where the appropriate balance lies is a subjective question.

For example, one may want to protect the property right holder in various situations where although the functionalities he can exercise in respect of the digital asset using his private key have not been diminished, his access to the digital asset has been denied or impeded. These situations do not involve burning or freezing, and are situations that do not necessarily yield a remedy under the existing law.

Situations where there has been a 'denial of access' without diminishing the functionalities the right holder can exercise using his private key include a distributed denial of service (DDoS) attack that prevents him from being able to access his digital asset. This

---

<sup>35</sup> See e.g. *Hedley Byrne & Co Ltd v Heller & Partners Ltd* [1963] UKHL 4, [1964] AC 465; *Spring v Guardian Assurance plc* [1994] UKHL 7, [1995] 2 AC 296; *Smith v Eric S Bush* [1990] UKHL 1, [1990] 1 AC 831; *White v Jones* [1995] UKHL 5, [1995] 2 AC 207; Goudkamp and Nolan (n 21 above), 5-049.

would happen for example if the claimant's private key is stored on a particular website and/or mobile application that is the subject of the DDoS attack.<sup>36</sup> Another example would be where there is a DDoS attack on blockchain network nodes that prevents the claimant from being able to access his asset for a substantial period of time.<sup>37</sup> There could also be a DDoS attack on the relevant application programming interface ('API') that connects the front-end application or website (used by the claimant to access his digital assets) with the blockchain back-end architecture, meaning that the claimant would be unable to access his digital asset through the application or website.

There is no default remedy under existing law in these situations.<sup>38</sup> Yet, in certain circumstances that involve a denial of access, one may argue that there should be liability. Denial of access via a DDoS attack, coupled with a mental state of intention,<sup>39</sup> may be a situation where many people would want to impose liability, because it involves a total impairment of use and the most egregious mental state.<sup>40</sup> This would be another area where the current law arguably leaves a gap in protection.

One may also think that there is a gap in protection where someone intentionally slows down the verification process of the blockchain nodes, leading to a slower rate at which blockchain transactions are processed. This would impair the use of someone's digital asset insofar as they cannot complete a blockchain transaction as quickly.

---

<sup>36</sup> As the private key is stored on such an application, a denial of service attack that prevents the claimant from accessing the application means that the claimant would not be able to access the private key and thus access his assets, assuming he does not keep a copy of the private key.

<sup>37</sup> This kind of attack does not need to involve any on-chain action: a regular botnet DDoS attack can achieve the same effect.

<sup>38</sup> There is no default claim under any of the causes of action mentioned in Section 2.3 above, for reasons that are similar to those given in Section 2.3 above.

<sup>39</sup> I.e. the defendant intending the consequence (denying the claimant from being able to access their digital asset), while (1) not believing that he has the best property right, and (2) not believing that the person(s) with better property rights have consented to the relevant action(s). See Section 4.1.2 below for the mental element of intention.

<sup>40</sup> There would be liability under Article 14 of the DAL in such situations: see DAL, Articles 14(1) and 14(2)(c).

Nonetheless, one may say that there should not be liability if there is only a minor slowing down of the verification process, even if such an outcome was intended by the defendant, or in cases where the defendant was reckless as to this outcome (i.e. that he foresaw a risk of this outcome and unreasonably took such a risk).<sup>41</sup>

Ultimately, the size of the gap may be debated, but the bottom line is that there is a clear gap in protection that exists in relation to the intentional<sup>42</sup> burning and freezing of digital assets, and arguably in terms of certain types of denial of access or impairment of use of a digital asset.

## **2.5 Filling the gap**

At this point, it would be appropriate to explore the ways in which this gap should be filled.

There are two main ways in which this gap can be filled. The first way would be to extend the chattel torts such that they cover digital assets. The second way would be to introduce a new regime that specifically deals with digital asset interferences and the recovery of control of a digital asset. It is suggested that the second option provides the best path forward to fill the gap.

The two options will be explored in turn.

### **3. Option 1: Extending the chattel torts**

The first possibility would be to extend the chattel torts (conversion, trespass and reversionary injury) to digital assets.

---

<sup>41</sup> Recklessness is explored in more detail in Section 4.1.2 below.

<sup>42</sup> Intention as defined in Section 4.1.2 below.

### 3.1 The argument in favour of extending the chattel torts

It has been argued by various academics that the tort of conversion should be extended to cover digital assets.<sup>43</sup> Similarly, the Law Commission in their Consultation Paper noted that there is a “good argument for extending the tort of conversion”<sup>44</sup> to digital assets.<sup>45</sup> This is on the basis that digital and physical assets are similar enough<sup>46</sup> such that it would be arbitrary not to subject them to the same interference regime. Without such an interference regime being applicable to digital assets, owners and holders of digital assets would be insufficiently protected.

Although the arguments have focused specifically on the tort of conversion, it is not only conversion that needs to be extended to cover digital assets if the full spectrum of ‘equivalent’<sup>47</sup> interferences<sup>48</sup> are to be covered. The other ‘property torts’ or ‘chattel torts’ of trespass and reversionary injury would also need to be extended to cover digital assets.<sup>49</sup>

The argument that conversion should be extended to intangible assets has been commonly made.<sup>50</sup> In respect of digital assets specifically, this argument has chiefly taken the form of the ‘anomaly’ argument. Specifically, since both physical and digital assets can be

---

<sup>43</sup> See e.g. Sarah Green and Ferdisha Snagg, ‘Intermediated Securities and Distributed Ledger Technology’, in Louise Gullifer and Jennifer Payne (eds), *Intermediation and Beyond* (Hart Publishing, 2019) 337, 345-348. This is a logical implication of an earlier argument made by Sarah Green and John Randall that conversion should cover “digitised products” such as software (which is ‘excludable’ and ‘exhaustible’): Sarah Green and John Randall, *The Tort of Conversion* (Hart Publishing, 2009), 118-128 (and see text to nn 53-55 below for excludability and exhaustibility). Also see Tatiana Cutts, ‘Possessable Digital Assets: Response to the Electronic Trade Documents Law Commission Consultation Paper No 254 and Call for Evidence on Digital Assets 2021’ (2021) LSE Law Policy Briefing Paper No.47, 5-6.

<sup>44</sup> Law Commission of England and Wales, *Digital Assets: Consultation paper* (Law Com No 256, 2022), 19.104; also see 19.89-19.123.

<sup>45</sup> Nonetheless, the Law Commission ultimately did not recommend an extension of conversion to digital assets: see discussion at Section 3.2 (text to nn 66-69) below.

<sup>46</sup> In the sense that they are (*inter alia*) independent of the legal system and can be transferred and are capable of exclusive control.

<sup>47</sup> E.g. less severe interferences (such as partial and more minor impairments of use that are nonetheless unauthorised). I am also using ‘equivalent’ in a loose sense: it is difficult to find the digital equivalent of a physical interference. See section 3.4.1 below.

<sup>48</sup> And interests (i.e. including reversionary interests).

<sup>49</sup> Trespass covers less severe interferences and reversionary injury covers interferences that affect the holder of a reversionary interest who does not have a right to immediate possession: See Section 3.3.1 below.

<sup>50</sup> See e.g. Green and Randall (n 43 above), chapter 5; Sarah Green, ‘Theft and conversion – tangibly different?’ (2012) 128 LQR 564; Susannah Lei Kan Shaw, “Conversion of Intangible Property: A Modest, but Principled Extension? A. Historical Perspective” (2009) 40 VUWLR 419.

stolen, transferred,<sup>51</sup> and are objects independent of the legal system, it would be anomalous to treat them differently. If misappropriating an iPhone (in a way that the claimant can no longer access it) constitutes conversion, so should misappropriating Bitcoin (in the form of an unauthorised transfer to a different blockchain address, such that the claimant can no longer access it). The similarity between physical and digital assets has been noted by the Law Commission as well as various academic commentators<sup>52</sup> who make the argument that both types of asset should be treated in like manner for the purpose of conversion (and presumably also the other chattel torts).<sup>53</sup>

Green and Snagg for example argue that there has been an over-emphasis on tangibility, noting that tangibility is merely a proxy for the distinction between ‘abstract’ and ‘concrete’ things: “tangibility historically *described* those things that were concrete, but it does not follow that it had any determinative influence on that categorisation”.<sup>54</sup> The normatively significant distinction for the law’s purposes is that between ‘abstract’ and ‘concrete’ things. ‘Abstract’ things do not have an existence independent of the legal system and relationships between individuals (e.g. debts), but ‘concrete’ things do have such an existence (e.g. tables, chairs, and cryptosecurities).<sup>55</sup> It is this distinction (as opposed to the distinction between tangibility and intangibility) that should be determinative in deciding whether the chattel tort regime applies to a particular type of asset.

---

<sup>51</sup> I.e. factually transferred from ‘space’ to ‘space’.

<sup>52</sup> See e.g. Green and Snagg (n 43 above).

<sup>53</sup> See e.g. *ibid*, 344-348. Green and Snagg refer only to conversion, but it would seem anomalous on their reasoning to exclude trespass and reversionary injury. Excluding the latter two torts would (1) provide no protection for lesser acts of impairment that do not constitute conversion, and (2) prevent reversionary owners from recovering for interferences that would constitute conversion if committed against the ‘immediate’ owner. Indeed, Green and Snagg mention other consequences that arise from cryptosecurities being capable of possession: for example they would “be amenable to bailment”, and “hav[e] the characteristic of negotiability” (348), so it would seem anomalous to exclude the possession-dependent consequence of being amenable to the torts of trespass and reversionary injury. Also see Law Commission, *Consultation Paper* (n 44 above), 19-101-19.104 (though their stance is more tentative: they state that “there is a good argument for extending the tort of conversion to data objects” (19.104) and that “there are good policy arguments for the extension of the tort of conversion to data objects” (19.103)).

<sup>54</sup> Green and Snagg (n 43 above), 346 ; also see Green and Randall (n 43 above), chapter 5.

<sup>55</sup> Green and Snagg (n 43 above), 346-347. Cryptosecurities are the main focus of Green and Snagg’s article.

This is because concrete things, unlike abstract things, are ‘excludable and exhaustible’ in the sense that they can be lost and stolen (hence are ‘exhaustible’)<sup>56</sup> and are capable of exclusive control (hence are ‘excludable’) regardless of whether a legal system exists and regardless of whether anyone claims rights in relation to them.<sup>57</sup> If an asset is excludable and exhaustible, “it can be possessed in a legal sense”.<sup>58</sup> This therefore allows one to group digital assets together with chattels insofar as both types of assets are ‘concrete’ things,<sup>59</sup> thus bringing in the protections of the chattel torts.<sup>60</sup> As such, the chattel tort regime should apply to digital assets (which are ‘concrete’ things).

Furthermore, other jurisdictions apply the chattel torts to intangibles: for example in the US there are cases applying conversion and trespass to digital assets.<sup>61</sup> Some US jurisdictions (as well as Canada and New Zealand) also apply conversion in the context of non-crypto ‘digital assets’<sup>62</sup> such as digital files and domain names.<sup>63</sup>

### **3.2 The three reasons why the chattel torts should not be extended to digital assets**

However, it is suggested that the argument for extending the chattel torts to digital assets is insufficiently focused on the big picture. This is for three reasons.

---

<sup>56</sup> *ibid*, 347.

<sup>57</sup> *ibid*, 346.

<sup>58</sup> *ibid*, 346.

<sup>59</sup> They discuss DLT cryptosecurities but the implication of their argument is that the tort should also apply to digital assets generally.

<sup>60</sup> See n 50 above.

<sup>61</sup> See n 227 below.

<sup>62</sup> Some use the term ‘digital assets’ in a wider sense to encompass assets that are duplicable and non-rivalrous, such as domain names and digital files.

<sup>63</sup> See e.g. *Kremen v Cohen* 337 F.3d 1024 (9th Cir., 2003); *Canivate Growing Systems Ltd v Brazier* [2020] BCSC 232; *Henderson v Walker* [2019] NZHC 2184. There are also trespass to chattels cases in the digital context, for example in the case of spam: see e.g. *CompuServe v Cyber Promotions* 962 F Supp 1015 (SD Ohio 1997). However, these cases are insufficient to establish that the chattel torts should be extended to digital assets, and do not detract from the arguments in this article: see Section 3.6.4 below.

First (and most fundamentally), physical and digital assets are very different in their nature, behaviour and respective environments, meaning that the concepts and thresholds used in the chattel tort context cannot be usefully applied in the digital asset context. This, coupled with the fact that digital assets are an asset class that judges tend to be substantially less familiar with,<sup>64</sup> creates uncertainty and a very substantial risk of producing the wrong normative result.<sup>65</sup>

Both the Law Commission<sup>66</sup> and the DIFC believe that conversion and/or the chattel torts should not be applied to digital assets, because the two types of assets are so fundamentally different. The Law Commission<sup>67</sup> note that chattels and digital assets “behave in different ways”,<sup>68</sup> such that applying conversion in the digital asset context would not be desirable.<sup>69</sup> Similarly, in the DAL Consultation Paper, the DIFC note that physical and digital assets are “very different in nature and surrounding environments”,<sup>70</sup> meaning that it is difficult to avoid

---

<sup>64</sup> As compared to physical assets.

<sup>65</sup> The phrases ‘wrong normative result’, ‘wrong normative threshold’ and ‘wrong normative balance’ are used often throughout this article. By these phrases, I am referring to an outcome that produces an overly narrow or overly wide scope of liability, or both (as a rule may be under-inclusive in some respects and over-inclusive in other respects). This is problematic because it results in claimants and defendants being underprotected or overprotected, or both. Indeed, as the scope of liability determines the scope of actions that defendants can take without incurring legal liability, the number of people to which they may be liable, and the extent to which they are so liable, having an overly wide scope of liability negatively affects the liberty of defendants. Similarly, having an overly narrow scope of liability results in claimants having insufficient rights.

Common causes of a wrong normative result include (1) reasoning that conflates conceptual distinction(s), treating relevant distinctions as irrelevant, and (2) treating irrelevant features as being relevant to the conclusion being reached. These causes broadly correspond with mistakes 1-6 in Section 3.6 below. Of course, features (1) and (2) can also exist without the wrong normative result being produced, but they entail messy or incorrect reasoning that carries negative knock-on effects on the clarity of the law. This messy or incorrect reasoning may also affect the reasoning and/or results of future cases, which may well draw on such messy or incorrect reasoning.

<sup>66</sup> In their Final Report: Law Commission of England and Wales, *Digital Assets: Final report* (HC 1486, Law Com No 412, 2023), 9.76.

<sup>67</sup> Citing my SSRN article (Hin Liu, ‘Interference torts in the digital asset world’ (2023) available at <https://ssrn.com/abstract=4433956> (accessed 16<sup>th</sup> September 2023)), which is an earlier version of my forthcoming Cambridge Law Journal article (Liu, ‘Interference torts’ (n 17 above)).

<sup>68</sup> Law Commission, *Final Report* (n 66 above), 9.73.

<sup>69</sup> *ibid*, 9.76.

<sup>70</sup> Dubai International Financial Centre, *Consultation Paper No. 4 (September 2023) Digital Assets Law* (2023), para 91.

“creating unacceptable uncertainty or substantially increasing the risk of incorrect decisions”<sup>71</sup> if the chattel torts were to be applied to digital assets.

Second, the chattel tort rules themselves are unsatisfactory, needlessly complex, and create problems for innocent defendants, and so applying such rules across to digital assets will mean that these negative characteristics will be replicated in the digital asset interference context.<sup>72</sup>

Third, the combination of the two above factors creates a very substantial risk of seven types of mistakes being made by judges (such as treating irrelevant elements of an asset as relevant (and vice versa), false analogies, opaque reasoning, and knock-on effects on the physical asset threshold).<sup>73</sup>

In order to contextualise the three substantive arguments as to why the chattel torts should not be extended to digital assets, it would be useful to set out the general structure and elements of an interference with a physical asset.

### **3.3 The interference regime for physical assets**

There is a general structure to every ‘interference’ with a physical asset. First, there is an action taken by the defendant. Second, the action impacts the claimant’s asset or his use of the asset (the ‘impact’). Third, the link between the action and the impact is proximate enough (‘causation’).<sup>74</sup> Fourth, the defendant also has a mental state when he performs the relevant

---

<sup>71</sup> *ibid*, para 91.

<sup>72</sup> The DIFC cites my SSRN article (Liu (n 67 above)), and notes that the existing chattel tort regime is “unsatisfactory and needlessly complex”, such that if it were to be extended to digital assets, the same “undesirable features [would be] replicated in the [d]igital [a]sset context”: see DIFC, *Consultation Paper* (n 70 above), para 91. See also Chapter 2, Section 3.2.1.2 above.

<sup>73</sup> There are seven types of possible mistakes: see Section 3.6, para 2 below.

<sup>74</sup> Sometimes there is no but-for causation, e.g. in the case of subsequent converters. But-for causation is not necessary to establish liability in conversion: “the court may treat wrongful conduct as having sufficient causal connection with the loss for the purpose of attracting responsibility even though the simple ‘but-for’ test is not satisfied”: *Kuwait Airways Corp v Iraqi Airways Co (Nos. 4 and 5)* [2002] UKHL 19, [2002] AC 883, at [74]

action. Finally, we need to look at what constitutes a defence to the cause of action, even if the first four elements are satisfied.

In order to ascertain whether the chattel tort regime can be transposed into the digital asset context, we need to analyse the five elements in respect of physical asset interferences, and determine the consequences of applying the same threshold to digital assets.

The five elements will be explored in turn.

### ***3.3.1 Elements 1 and 2: Action of the defendant and impact on the claimant's asset or use of his asset***

The first two elements will be discussed together because in the context of the chattel torts, element 1 (the action of the defendant) forms part of the definition of element 2 (the impact on the claimant or his asset).

The duty on the defendant consists of a duty not to (deliberately) physically interfere with the claimant's asset.<sup>75</sup> In the context of elements 1 and 2, the requirement that the defendant must not 'physically interfere' with the claimant's asset can be broken down into a few sub-duties. First, he must not take any deliberate positive action that physically damages the claimant's chattel. Secondly, he must not make any deliberate physical contact with the asset (which may happen through using his own body or through other means such as through an object). Third, he must not completely impair the claimant's use of his asset (irrespective of

---

(Lord Nicholls). See also Simon Douglas, 'The nature of conversion' (2009) 68(1) CLJ 198, 222, and n 84 below

<sup>75</sup> 'Deliberately' i.e. deliberate act of interfering with the chattel, as opposed to having any knowledge that the chattel is not theirs.

whether there has been any physical contact or damage).<sup>76</sup> Fourth, he must not enter into a transaction that deprives the claimant of his title to the asset.<sup>77</sup>

These four duties are covered by the three torts of conversion, trespass and reversionary injury.

Conversion covers the most severe types of interference. Specifically, it requires a deliberate action by the defendant that either (a) physically damages the chattel (or involves physically touching the chattel) in a way that totally or severely excludes the claimant from use of the chattel<sup>78</sup> (even for a temporary period),<sup>79</sup> or (b) directly excludes the claimant from using the chattel (for any period of time) despite a lack of physical contact or damage. Examples of (a) would include taking, selling,<sup>80</sup> or destroying the asset, or detaining the asset with an intention to assert title,<sup>81</sup> or transforming the asset in a way that it loses its essential identity.<sup>82</sup> In terms of (b), this includes a sale that deprives the claimant of his title,<sup>83</sup> and this results in a ‘total exclusion of use’ in the sense that the claimant’s use of the asset would involve the incurring of a liability to the new owner (given that he no longer has title).<sup>84</sup>

---

<sup>76</sup> *Burroughes v Bayne* (1860) 5 H & N 296; Simon Douglas, ‘Actionable Interferences in the Chattel Torts: A New Perspective on Economic Loss’ in Simone Degeling, James Edelman, James Goudkamp (eds), *Torts in Commercial Law* (Routledge, 2011), 87, 95-96.

<sup>77</sup> By way of sale: see Jones et al (n 23 above), 16-22.

<sup>78</sup> Examples where the claimant’s use of the asset is severely (but not totally) excluded would include adulteration of wine (*Richardson v Atkinson* (1723) 1 Stra 576; 93 ER 710), or arguably a “transformation of goods so that they lose their essential identity” (see Michael Bridge, Louise Gullifer, Kelvin Low, Gerard McMeel, *The Law of Personal Property* (3<sup>rd</sup> ed, Sweet & Maxwell 2021), 33-019).

<sup>79</sup> *England v Cowley* (1873) LR 8 Exch 126.

<sup>80</sup> Specifically, selling the asset in an unauthorised way that involves physical contact with the good (the obvious example would be delivery of the asset to the buyer).

<sup>81</sup> In detention cases, the defendant is entitled to “adequate time to inquire into the rights of the claimant”: *Clayton v Roy* [1911] 2 KB 1031 at 1051. As such, the defendant is not liable for the detention *per se* but a detention coupled with an intention to assert title: Bridge et al (n 78 above), 33-032 and fn179.

<sup>82</sup> Bridge et al (n 78 above), 33-019 (transformation of the good so that it loses its essential identity).

<sup>83</sup> Specifically, a sale that does not involve delivery or physical contact. See Jones et al (n 23 above), 16-22 (discussing *nemo dat* exceptions).

<sup>84</sup> For conversion there is no but-for causation requirement. Thus, if X takes C’s goods without C’s permission, and D takes the same good from X without C’s or X’s permission, D is liable in conversion, despite the fact that but-for D’s taking, C would still have been excluded from using his good – D’s act itself excludes C from using the asset. In the ‘proximity/causation’ section (Section 3.3.2 below) I discuss the intervening acts issue as opposed to the but-for causation issue (since there is no but-for causation constraint on the defendant’s liability).

Indeed, partial impairments of use do not constitute conversion in the absence of physical contact, as demonstrated by *Club Cruise*.<sup>85</sup> In *Club Cruise*, an official served an administrative detention notice on the claimant shipowner, mandating its ship to stay in port. The detention notice turned out to be invalid, and the claimant sued in conversion. The court held that there was no conversion, since there was no physical contact or restraint, and the claimant still had possession of the ship.

Trespass requires intentional action by the defendant that physically touches or damages the chattel (and covers lesser interferences that are not serious enough to amount to conversion).<sup>86</sup>

Nonetheless, a person can only sue in conversion if he had actual possession or a right to immediate possession of the chattel at the time of the interference, and can only sue in trespass if he had possession of the chattel at the time of the interference.<sup>87</sup> As such, many people with a ‘reversionary’ interest in a chattel (e.g. a pledgor or a term bailor) would not be able to sue in conversion or trespass.

This is where the tort of reversionary injury becomes relevant. It covers any act that would constitute conversion, trespass (or negligence), but also requires actual damage,<sup>88</sup> and is only available to someone who has a ‘reversionary’ interest in a chattel. A person with a reversionary interest will be able to sue in reversionary injury if there has been damage to *his* interest, as opposed to damage to merely the pledgee or bailee’s interest.<sup>89</sup>

---

<sup>85</sup> *Club Cruise Entertainment v Department of Transport* [2008] EWHC 2794 (Comm), [2009] 1 All ER (Comm) 955.

<sup>86</sup> See e.g. Douglas (n 76 above), 88–92. Nonetheless, the authors of *Clerk and Lindsell on Torts* suggest that there should be no liability in trespass where the defendant’s conduct has not “gone beyond generally acceptable standards of conduct” (citing *Collins v Wilcock* [1984] 1 WLR 1172, 1178), such as where a pedestrian picks up a parcel that has been dropped by another person and returns it to him: Jones et al (n 23 above), 16-134.

<sup>87</sup> Jones et al (n 23 above), 16-43 and 16-139.

<sup>88</sup> *ibid*, 16-151.

<sup>89</sup> *HSBC Rail (UK) Ltd v Network Rail Infrastructure Ltd* [2006] 1 WLR 643. See also Jones et al (n 23 above), 16-146: the act needs to have “the effect of depriving him either temporarily or permanently of the benefit of his reversionary interest”.

It is worth noting that not every ‘impairment’ or ‘change in form’ amounts to an actionable interference. For example, Douglas gives the example of a person who buys up all the local supplies of petrol.<sup>90</sup> This would lead to people’s use of their cars being impaired, as the cars would not have fuel anymore and so people would not be able to drive their cars. However, this impairment is not an ‘interference’ for the purpose of the chattel torts, because if such an action attracted liability in the chattel torts, this would unduly limit the liberty of defendants.<sup>91</sup>

Overall, ‘physical contact or physical damage’ is a requirement for trespass, and for conversions that do not amount to a total impairment of use. It is also a requirement for the ‘equivalent’ reversionary injury claim,<sup>92</sup> provided there is actual damage to the reversionary interest.<sup>93</sup> If there is no physical contact with or physical damage to the chattel, the ‘conduct’ requirement is increased (i.e. there must be a total impairment of use before there can be an interference).<sup>94</sup> Nonetheless, in most physical asset interference cases, physical contact or damage usually exists.

### ***3.3.2 Element 3: Proximity/causation***

There is a ‘directness’ requirement for trespass,<sup>95</sup> meaning that there is a ‘causation’ constraint that limits the defendant’s liability. A defendant does not commit trespass if he lays a trap for a

---

<sup>90</sup> Douglas (n 76 above), 92.

<sup>91</sup> There are various restrictions on a claimant’s ability to recover for pure economic losses, which are carefully policed to prevent potential defendants from being exposed to too much liability. For example, inducing breach of contract requires knowledge that the course of conduct would amount to a breach of contract, plus an intention to procure such a breach: See Jones et al (n 23 above), 23-32-23-38. Causing loss by unlawful means requires an intention to cause loss to the claimant: 23-81.

<sup>92</sup> By the ‘equivalent’ claim, I am referring to situations where someone is suing for damage to their reversionary interest, there is no total impairment of use of the chattel, and they are suing for what would otherwise amount to a trespass or a conversion.

<sup>93</sup> Reversionary injury requires actual damage (see Jones et al (n 23 above), 16-146).

<sup>94</sup> Douglas (n 76 above), 95-96.

<sup>95</sup> Jones et al (n 23 above), 16-133; Bridge et al (n 78 above), 33-004.

physical object to fall into.<sup>96</sup> As such, situations that potentially engage the ‘intervening acts of causation’ debate are outside the scope of the tort.

In respect of conversion, the types of actions that constitute the tort all involve a very direct causal chain (e.g. taking or destruction of an asset).<sup>97</sup> There is no intervening act between the defendant’s action and the impact on the claimant (or his asset), because the acts that involve conversion involve one of two patterns, both of which do not involve any act in between the defendant’s action and the impact on the claimant (or much time in between). First, there are cases involving direct contact with the chattel (where the defendant’s action and the impact on the asset happens at the same time (or almost at the same time)).<sup>98</sup> Second, there are cases involving a total exclusion of the claimant’s use of the chattel without any act in between the defendant’s action and the claimant’s exclusion from use (such as *Burroughes v Bayne*).<sup>99</sup> As such, the ‘intervening acts of causation’ debate is not relevant in the conversion context.<sup>100</sup>

These ‘causation’ principles also apply in respect of reversionary injury, as the tort covers the same ground as conversion and trespass<sup>101</sup> insofar as deliberate interferences are concerned,<sup>102</sup> provided that a reversionary interest is damaged.<sup>103</sup>

### **3.3.3 Element 4: Mental requirement**

---

<sup>96</sup> This would be too ‘indirect’ to count as trespass. see also Bridge et al (n 78 above), 33-004: there is no trespass claim against a “defendant who, instead of feeding poisoned meat directly to the claimant’s dogs, lays it down for them to find it”; *Hutchins v Maughan* [1947] VLR 131 at 134.

<sup>97</sup> Or there may not even be but-for causation, for example in the case of a subsequent converter: the defendant’s action excludes the claimant from use of his chattel but the exclusion would still have occurred without the defendant’s action.

<sup>98</sup> E.g. where the defendant takes the claimant’s chattel.

<sup>99</sup> *Burroughes* (n 76 above).

<sup>100</sup> For the purposes of *liability* in conversion. Some ‘causal chain’ issues (such as mitigation) are relevant at the remedies stage: see e.g. Bridge et al (n 78 above), 33-053.

<sup>101</sup> Jones et al (n 23 above), 16-146.

<sup>102</sup> Reversionary injury also covers negligent interferences with a reversionary interest (*ibid*, 16-151) but the focus here is on deliberate interferences.

<sup>103</sup> Actual damage is required: *ibid*, 16-146.

Conversion and trespass (as well as the equivalent wrongs in respect of reversionary interests) impose strict liability.<sup>104</sup> This has been criticised on the basis that it is overly harsh on defendants and does not provide fair warning,<sup>105</sup> but one could also justify it on the basis that elements 2-3 are narrowly constrained. Specifically, because ‘physical contact or physical damage’ is a requirement where there is no total impairment of use, this provides some degree of fair warning. The boundaries of the physical thing provide a crucial limit to the potential scope of liability,<sup>106</sup> which reduces (or eliminates) the need for liability to be constrained by way of a mental requirement.

### **3.3.4 Element 5: Defences**

There are various specific statutory defences to the chattel torts,<sup>107</sup> and in terms of general common law, the main defence is consent.<sup>108</sup> If the claimant expressly or impliedly consents to the interference, the defendant has a defence.<sup>109</sup>

## **3.4 Argument 1: Difficulty in applying chattel tort elements and normative balance to digital assets**

The most fundamental reason why the chattel torts should not be applied to digital assets is that there are many significant differences between the nature, behaviour and environments of

---

<sup>104</sup> This means that the defendant would be liable irrespective of the reasonableness of his behaviour. He just needs to intend the act constituting the interference.

<sup>105</sup> See Section 3.5.3 below.

<sup>106</sup> See e.g. Simon Douglas and Ben McFarlane, ‘Defining Property Rights’ in James Penner and Henry Smith (eds), *Philosophical Foundations of Property Law* (OUP, 2013) 219, 239.

<sup>107</sup> See e.g. Jones et al (n 23 above), 16-81-16-87. E.g. Torts (Interference with Goods) Act 1977, s.8(1); Insolvency Act 1986, ss.234(3), 307(4) and 346(7); Cheques Act 1957, s.4.

<sup>108</sup> There are other common law defences based on ministerial handling, as well as based on the bailee acting on the bailor’s orders: see Jones et al (n 23 above), 16-77, 16-78. There is also the defence of illegality: *ibid*, 16-88.

<sup>109</sup> See e.g. Bridge et al (n 78 above), 33-009.

physical and digital assets. As a result, existing concepts that are used to resolve disputes in the physical asset context are not adequate to resolve disputes in the digital asset context.

There are various differences between physical and digital assets that are worthy of note. First, a physical asset has a distinct molecular boundary that defines the space that it occupies, whereas a digital asset has no distinct molecular boundary. Second, the blockchain environment is an ‘opt-in’ environment that one has the option not to join, whereas the physical environment is something that we are part of no matter what. Third, the blockchain environment is ‘composable’ in the sense that coders can define the features of the ‘blockchain world’ they create to a much greater degree than a person in the physical world can define the features of the assets they create.<sup>110</sup> Fourth, a digital asset can only be ‘accessed’ through a digital device, whereas a physical asset can be accessed by making contact with the (physical) space in which it is contained.

Fifth, we have a much better idea of how physical assets work and behave, given that we interact with them on a daily basis, and they occupy a molecular space that our senses are attuned to, meaning that we can spot dangers arising out of them using our senses (primarily vision and touch). This stands in contrast with digital assets where we are unable to spot similar dangers, given that the code-governed environment is unfamiliar to most people and many impairments may occur outside our knowledge or foresight.

Because of these differences, concepts that are adequate to resolve disputes in the physical asset context are not adequate to resolve disputes in the digital asset context. They do not yield determinate results<sup>111</sup> in the digital asset context: for example, in the case of concepts such as ‘physical interference’ or ‘physical contact’, the nature and environment of digital assets is such that no direct analogy with physical assets can be drawn.<sup>112</sup>

---

<sup>110</sup> Assets in the physical world are subject to the constraints of physical laws (gravity, friction etc).

<sup>111</sup> Or at least results that are determinate enough.

<sup>112</sup> See Section 3.4.1 below.

Yet, a judge still needs to make a decision on a given set of facts, and so he will need to try to find the equivalent of ‘physical interference’ or ‘physical contact’. However, there will not be a precise equivalent, and whichever ‘equivalent’ applied will (at best) be a rough approximation. We also do not know which approximation the judge will apply, given that there are many possible options (explored below).<sup>113</sup>

This creates an unacceptable amount of uncertainty for parties, given that they would find it extremely difficult to predict their legal positions (since each ‘proxy’ or ‘approximation’ generates a substantially different scope of liability),<sup>114</sup> and parties would need to litigate<sup>115</sup> to find out their legal positions.<sup>116</sup> This creates a substantial risk of a chilling effect on users of the blockchain<sup>117</sup> (including centralised exchanges, and operators of blockchains) as they may fear liability under the chattel torts if they take certain digital actions (and in particular, actions on the blockchain).<sup>118</sup>

Apart from the problem of uncertainty, there is a significant risk that judges will produce the wrong normative threshold by picking an inaccurate ‘equivalent’. Since digital assets are technically complex and thus difficult to understand, judges may be misled into using an inaccurate proxy that produces an overly wide or narrow scope of liability. Alternatively, judges may pick a proxy that can no longer be seen as an ‘equivalent’ to the corresponding chattel tort requirement, which effectively modifies the threshold in respect of the ‘chattel’ torts while paying lip service to the requirement in question.

---

<sup>113</sup> See Section 3.4.1 below. Because there is no direct equivalent, there are many possible ‘proxies’, but each ‘proxy’ generates a substantially different scope of liability.

<sup>114</sup> See Section 3.4.1 below.

<sup>115</sup> Or there must be a case that is relevant enough to the parties’ situation, e.g. one that involving facts that are very similar to the parties’ situation, and states the relevant rule in a way where it is clear enough what the outcome of the litigation would be.

<sup>116</sup> This puts defendants in a worse position than the ‘strict liability’ scenario in Section 3.5.3 below where one can in many circumstances be able to find out their legal position by verifying whether someone owns a good.

<sup>117</sup> Creating chilling effects in this way carries the undesirable effect of stifling useful economic activity and innovation/experimentation on the blockchain.

<sup>118</sup> Such as an exchange executing an on-chain transfer of an asset (to which it only has an inferior relative title) to a third party by transferring it to him on-chain, or a blockchain administrator freezing tokens in response to a suspected hack.

Judges may also produce the wrong normative threshold through directly applying the physical asset threshold to digital assets. This is because the differences in physical and digital assets (and their respective policies) justify different requirements, and applying the same requirement produces undesirable results in the digital asset context. An example that will be explored below relates to the role of digital asset ‘killswitches’ in the context of the ‘consent’ defence.<sup>119</sup>

### *3.4.1 No proxy for physical interference*

First, in the digital asset context, there is fundamentally no equivalent of or proxy for the ‘physical contact/damage’ requirement for trespasses, and for conversions that do not lead to a total impairment of use.<sup>120</sup>

Physical assets have physical boundaries (i.e. molecular boundaries), and the ‘physical contact/damage’ requirement provides a very important limit to the scope of liability, especially given that the chattel torts attract strict liability. It is relatively easy to identify whether there has been physical contact (touching of molecules that constitute the chattel) or physical damage (a change in the molecular structure of the chattel that renders the chattel less useful or valuable).<sup>121</sup> This also allows a clear distinction to be drawn between a ‘physical interference’ and an ‘impairment of use’: there can be one without the other.

There is no equivalent of ‘physical contact or physical damage’ to (or ‘physical interference’ with) a digital asset. A digital asset is ideational, and common ways in which ‘destruction’ or ‘denial or impairment of access’ occur include where the defendant causes (1)

---

<sup>119</sup> See Section 3.4.2 below.

<sup>120</sup> There is, however, no need to find a ‘proxy’ in case of total impairments of use (since there is no physical interference requirement for total impairments of use: see Section 3.3.1, paras 2, 4 and 10 above).

<sup>121</sup> See Douglas (n 76 above), 89: there needs to be harm to the “actual physical structure” of the chattel, and a mere impairment of use is insufficient to constitute physical damage.

the freezing of the asset, (2) a ‘denial of service’ attack, (3) a transfer of the asset to another address (whether it is a smart contract or wallet address, and whether it has a private key or not),<sup>122</sup> or (4) destruction of the asset through burning. There is no equivalent of a physical boundary that people can walk into and interact with, because of fundamental differences in the nature of physical and digital assets. These differences mean that unlike physical assets where one can cleanly distinguish ‘impairment of use’ and ‘physical interference’, one cannot cleanly distinguish ‘impairment of use’ of a digital asset from ‘digital interference with the asset’.

If one applies the physical damage/contact requirement<sup>123</sup> literally to digital assets, this will result in the claimant having no remedy in situations that involve freezing his digital asset in a way that partially impairs the use of his digital asset. This is because there is no physical damage/contact, which means there is no liability in trespass or conversion.

Nonetheless, are there any proxies that can serve as adequate substitutes for such a requirement? One possibility would be to limit actionable interferences to on-chain actions (as opposed to off-chain actions). This means that a defendant who does not take any action on the blockchain (e.g. calling a function)<sup>124</sup> would not be liable for interference. This to some extent mirrors the fact that if a defendant does not interact with or physically damage a chattel, he would not be liable in the chattel torts (unless there is a total impairment of use).

This in essence could be seen as underpinned by a ‘fair warning’ rationale that preserves the liberty of the defendant: one should interact with the blockchain at one’s own risk, but there is no liability if one does not interact with the blockchain. Similarly, with the chattel torts, the message is that one interacts with chattels at one’s own risk, but there is no liability if one does not interact with chattels (unless there is a total impairment of use).

---

<sup>122</sup> Burn addresses do not have private keys.

<sup>123</sup> Which would apply if there is no total impairment of use.

<sup>124</sup> Calling a smart contract function on the blockchain.

To approximate the chattel tort position further, this ‘on-chain interference’ requirement could be imposed in relation to partial impairments of use, but not for total impairments of use.

However, there are two problems with using an ‘on-chain interference’ requirement as a proxy. First, this requirement does not actually provide fair warning. Any on-chain function (when executed) may be a triggering condition for some other digital asset being burned or frozen.<sup>125</sup> To prevent this outcome, the defendant would need to search *all* of the smart contracts that exist and ensure that no digital asset would be burned or frozen as a result of executing/calling the intended function. Indeed, the analogy between ‘interacting with a physical asset’ and ‘interacting with a blockchain’ is a loose one. In the physical asset context, it is reasonably expected that one is supposed to ‘keep off’ a physical asset. This is because (1) the general expectation is that someone may (or is likely to) own it, and (2) one can avoid interacting with it because it has visible boundaries, meaning that a defendant can keep off it without expending much mental energy.<sup>126</sup> In contrast, interacting with a blockchain (even intentionally) does not (and ought not to) give rise to the expectation of ‘keep off any digital assets’, because (1) a digital asset has no visible boundaries and (2) it is difficult to conclusively avoid the outcome of a digital asset being burned or frozen as a result of an on-chain interaction.

Second, the ‘on-chain interference’ requirement would result in an under-inclusive rule that protects claimants insufficiently. For example, it would exclude a distributed denial of service (‘DDoS’) attack by a defendant (which can be an off-chain activity) that prevents the claimant from being able to access his digital asset. This would happen for example if the claimant’s private key is stored on a particular website and/or mobile application that is the

---

<sup>125</sup> Blockchain developers merely need to code this into their application as an if-then statement. They have an extremely high degree of freedom when building their applications on the blockchain: they can provide for any functionality that is compliant with the programming language used by the relevant blockchain (e.g. Solidity, in the case of Ethereum).

<sup>126</sup> Douglas and McFarlane (n 106 above), 239-240; Thomas W Merrill and Henry E Smith, ‘The Architecture of Property’ in Hanoch Dagan and Benjamin C Zipursky (eds), *Research Handbook on Private Law Theory* (Elgar, 2020) 134, 142.

subject of the DDoS attack.<sup>127</sup> Another example would be where there is a DDoS attack on blockchain network nodes that prevents the claimant from being able to access his asset for a substantial period of time.<sup>128</sup> There could also be a DDoS attack on the relevant application programming interface ('API') that connects the front-end application or website (used by the claimant to access his digital assets) with the blockchain back-end architecture, meaning that the claimant would be unable to access his digital asset through the application or website.

Another possibility would be to impose a 'directness' requirement for digital asset interferences, by analogy with the directness requirement in trespass to goods.

However, the analogy breaks down on a very fundamental level. With physical assets, we know *what* should be directly caused in the trespass context (i.e. the 'physical interference': physical contact or physical damage). In contrast, with digital assets, we do not know what should be directly caused (i.e. the impairment of use, the function call etc). Thus, imposing a directness requirement merely begs the question of what proxy we should use as an equivalent of 'physical interference', because we need to know what needs to be directly caused before the analogy with trespass can stand.

Nonetheless, could we use a 'directness' requirement to constrain the scope of actionable interference, even though we do not know what must be directly caused? It is suggested that a directness requirement is too vague. Directness usually means sufficient proximity in relation to the (1) time taken between the defendant's action and the relevant consequence, and (2) number of events between the action and the consequence, and also means that (3) the original action carries a high degree of influence in generating the relevant consequence.<sup>129</sup> However, these three elements are very open-ended, and are difficult to apply

---

<sup>127</sup> As the private key is stored on such an application, a denial of service attack that prevents the claimant from accessing the application means that the claimant would not be able to access the private key and thus access his digital asset(s), assuming he does not keep a copy of the private key.

<sup>128</sup> This kind of attack does not need to involve any on-chain action: a regular botnet DDoS attack can achieve the same effect.

<sup>129</sup> As opposed to e.g. a significant cause of the consequence being the voluntary action of C.

to digital assets since it is difficult to generate a determinate result purely from applying these criteria. For example, it is difficult to know the boundaries of each of the criteria,<sup>130</sup> and the weighting of each factor, and this creates room for judges to be able to instrumentally manipulate the criteria to reach a desired result, at the expense of the law's predictability and consistency.

Another proxy may be one based on the direct linguistic equivalent of '(intentional) physical contact': namely '(intentional) digital contact'. However, if 'digital contact' (i.e. interacting with a digital device or system) were to be the equivalent threshold, there would simply be no fair warning to potential defendants (especially since conversion is a strict liability tort).

This contrasts with the position as regards physical assets, because physical assets have a boundary (and so avoiding intentional physical contact or damage is relatively easy). It is (relatively) not a big ask to require a person not to intentionally make contact with physical objects in his proximity, not to perform intentional acts that lead to damage to physical objects, and not to perform intentional acts that lead to someone being totally excluded from using a physical object. Given these constraints, it may be argued that imposing strict liability provides a substantial degree of fair warning to defendants.<sup>131</sup>

By contrast, in the digital asset context, people intentionally interact with functions on-chain, and update data off-chain, in a way that may cause damage or destruction to digital assets without them knowing. It is difficult to know when one's conduct will lead to, e.g. damage or exclusion of access to a digital asset.

For example, in the context of the prediction markets, someone might deploy a smart contract for the purpose of a sports bet, and designate a website as the source of authority for

---

<sup>130</sup> E.g. what is the 'allowable time period' between the action and the damage/consequence?

<sup>131</sup> Nonetheless, the strict liability nature of conversion has been criticised for its harshness on innocent defendants: see Section 3.5.3 below.

the final score. Funds (in the form of digital assets) would be locked up in that smart contract (and could e.g. be jointly owned by all parties to the bet), and subsequently distributed to the person who wins the bet. The smart contract can designate any website as the ‘ultimate source of information’ for the final score, and the problem arises where such a website misreports the relevant score, causing the tokens to be distributed to the wrong person.

In this case, there is potential liability for causing the ‘diversion’ or ‘misappropriation’ of a digital asset. This liability could attach to the operator of *any* website that shows sports scores. It is difficult for the operator of any such website to know whether the information displayed on their website is being used for the purposes of a smart contract oracle. Extrapolating further, the same issues would apply to prediction markets more generally, and importantly in the context of financial derivatives.

When coupled with strict liability, the requirement of ‘digital contact’ would make people hypervigilant and lead to a waste of people’s mental energy on thinking about whether they may be liable, and may cause them to take preventive or defensive action. As such, their liberty (and economically useful activity) would be stifled. This position is similar to that in respect of pure economic loss, where a high mental requirement is imposed.<sup>132</sup> The law does not impose strict liability for causing pure economic loss, because doing so would stifle ordinary activity and make people hypervigilant.<sup>133</sup> Indeed, the ethos of the blockchain as an open-source environment where people are encouraged to experiment with code<sup>134</sup> should be respected: imposing strict liability in the blockchain environment would run directly counter to such an ethos.

---

<sup>132</sup> For example, inducing breach of contract requires knowledge that the course of conduct would amount to a breach of contract, plus an intention to procure such a breach: See Jones et al (n 23 above), 23-32 – 23-38. Causing loss by unlawful means requires an intention to cause loss to the claimant: 23-81.

<sup>133</sup> There would be potentially indeterminate liability.

<sup>134</sup> For example, composability is a crucial feature of the blockchain: people can use and combine existing code to create new applications.

### ***3.4.2 Blockchain environment/policy (v physical environment/policy)***

The blockchain environment is very different from the physical environment, and this means that the policies that are relevant in the blockchain world produce a different normative balance as compared to those in the physical world. This means that the scope of defences available (as well as the scope of prohibited actions) in respect of digital asset interferences are likely to be very different to that in respect of physical assets.

For example, there can be ‘killswitches’ and other coded permissions that are given to people so that they can (e.g.) burn or freeze an asset. If such people burn or freeze an asset with the intention of doing so, this would be an intentional action that directly leads to C’s use being impaired or destroyed (as he would not be able to transfer the asset, and - in the case of burning - not be able to access the asset as well). Such situations may arise for example if there has been a (reasonably) suspected bug or hack, and the developer/administrator exercises the killswitch to investigate what has been happening with the code, with the effect that the claimant is no longer able to use or access his asset at all.<sup>135</sup> This would constitute the equivalent of a physical conversion,<sup>136</sup> and there is no defence to conversion that applies here. The ‘consent’ defence would not apply in many (or most) instances since claimants in many (or most) instances would not even be aware of such a killswitch or permission,<sup>137</sup> and so there is no express or implied consent.<sup>138</sup> Also, even though the defendant may argue that the

---

<sup>135</sup> Under this specific example the claimant cannot access or use the asset at all. In other circumstances a freeze permission may be exercised but the claimant can still access certain functionalities in respect of the asset (e.g. the ability to sign a signature from the address in which the asset is contained, and/or exercise a voting right in respect of it).

<sup>136</sup> Here there would be a total impairment of use.

<sup>137</sup> In case there is any ambiguity, ‘permission’ here refers to the coded permission (the factual power to freeze or burn the asset that is given to the developer/administrator under the relevant code), as opposed to permission (consent) given by C in relation to the impairment of use.

<sup>138</sup> In general, people are not aware of killswitches or burn/freeze permissions in respect of a particular digital asset, because they do not read (or understand) the underlying code that contains such permissions, or any associated documents that may alert them to the possibility of such permissions. In this general scenario, there would be no actual (express or implied) consent to the exercise of such permission(s).

claimant opted into the blockchain world (and his particular protocol) and thus consented to its rules (or ‘logic’), this would not succeed. This is because such ‘logic consent’ does not involve actual consent (whether express or implied) nor perhaps even ‘hypothetical’ consent (i.e. where the claimant would have consented if he was made aware of the effect of the protocol rules).

Furthermore, the necessity defence (if it applies to conversion at all)<sup>139</sup> does not cover situations where there is no actual danger to an asset.<sup>140</sup> Thus, it does not cover situations where the developer or administrator exercises a killswitch under a reasonable suspicion that assets on the blockchain are in danger of being (e.g.) taken or burned, when that danger does not in fact exist. This situation could arise if the developer or administrator acts on an alert raised by an intrusion detection system (IDS)<sup>141</sup> that is a ‘false positive’, i.e. where the alert does not correspond with an actual danger.

However, there is a strong argument that this is the wrong normative result,<sup>142</sup> and that a defence ought to be available in (at least some) such circumstances. First, this is because the killswitch/permission was constructed as part of the blockchain environment. It was deliberately created (i.e. the effect was intended), as opposed to being an accidental consequence of bad programming.

A particular blockchain environment can be constructed in a multitude of ways, and one can create the rules that govern such a blockchain environment/application. This stands in

---

<sup>139</sup> There is case law suggesting that the necessity defence applies to trespass: see *Cope v Sharpe (No 2)* [1912] 1 KB 496; *Kirk v Gregory* (1876) 1 Ex D 55; *Sorrell v Paget* [1950] 1 KB 252, but there appears to be no case law applying it to conversion. In general, opinions are divided as to whether there is a defence of private necessity: see e.g. James Goudkamp, *Tort Law Defences* (Hart Publishing, 2013), 114 (no defence of private necessity); John Goldberg, ‘Tort Law’s Missing Excuses’ in Dyson et al (eds), *Defences in Tort* (Hart Publishing, 2015) 53 (no defence of private necessity); cf Graham Virgo, ‘Justifying Necessity as a Defence in Tort Law’ in Dyson et al (eds), *Defences in Tort* (Hart Publishing, 2015) 135, 155, where his view is that apart from the tort of negligence, “necessity is...a defence to all other torts”).

<sup>140</sup> *Monsanto plc v Tilly* [2000] Env LR 313, [54]; Virgo (n 139 above), 156.

<sup>141</sup> An intrusion detection system is an application that monitors network activity, searches for cybersecurity threats and suspicious activity, and issues alerts when such threats or suspicious activity is detected.

<sup>142</sup> Specifically that there is too much liability on the defendant.

contrast with the physical environment where the physical laws are relatively fixed/immutable. As such, if a blockchain developer decides to design a blockchain that includes a killswitch that is intended to be used in circumstances where the assets are in danger of imminent misappropriation or destruction by a hacker, or in danger of being destroyed by an unintended bug, or where there is a reasonable suspicion of such danger(s), affording no defence to the developer where those precise circumstances exist (despite the lack of consent from the claimant) may be thought to be unfair. This is because it frustrates the very purpose of the developer's deliberate design choice to add in a killswitch to protect the integrity of the blockchain.<sup>143</sup>

Also, a blockchain environment is an opt-in environment (in the sense that a person can choose whether to engage with it or not), unlike the physical environment (which every person has no choice but to engage with). If one chooses to enter a blockchain environment, it would seem fair to suggest that in certain circumstances within people's reasonable expectations,<sup>144</sup> those with killswitch/burn permissions should be allowed to exercise their power to transfer/freeze assets as intended by the design of the blockchain.

However, a claimant is not reasonably expected to look out for his 'blockchain environment' in the same way that he is expected to look out for his physical environment. Looking out for one's physical environment merely requires one to be (visually and kinaesthetically) attentive to one's surroundings, which is already habitual for most people and thus does not take much effort. In contrast, looking out for one's blockchain environment carries vastly higher information costs, as it requires a detailed understanding of code (which

---

<sup>143</sup> When the integrity of the blockchain is under threat, this creates the potential for a lot of harm, and the harm that would otherwise be caused by the bug or hack would often be much greater than the harm caused to the claimant's asset whose use is (non-consensually) impaired as a result of using the killswitch. This is because many people can be affected at once by such hacks and bugs, a large amount of high value assets can be quickly misappropriated or drained, further damage could be done to the blockchain and internal company operations, and limiting the (potential or actual) damage from these hacks and bugs is a time-sensitive task.

<sup>144</sup> Such as where there is an imminent danger of a hack that significantly threatens the security of the assets on the relevant blockchain.

the vast majority of people do not have) as well as the ways in which it could malfunction. Indeed, even programmers cannot anticipate all bugs/loopholes in the code, so it would be extreme to suggest that an average user of the blockchain should be expected to do so. Thus, if the particular use of a killswitch is outside a claimant's reasonable expectations, a defendant in general ought not to be afforded a defence.

In general, it is suggested that a defence should be afforded in a wider range of situations in the digital asset context because (1) the need to reverse the effect of hacks and bugs is a very time-sensitive task, and (2) the initial signs of a hack or bug can be difficult to distinguish from legitimate or normal conduct in the digital world.

Hacks or bugs that interfere significantly with digital assets (or their use), including hacks that cause complete impairments of use, typically happen in seconds. For example, a hack that drains a smart contract of its assets can happen in seconds,<sup>145</sup> and such a smart contract may contain millions of dollars of assets. These two factors (high speed and high monetary value) mean it is absolutely critical to minimise the occurrence (and consequences) of these hacks and incidents.

At the same time, the initial signs that lead up to a hack or bug can look very similar to legitimate conduct on the blockchain or internet (e.g. a high number of requests or transactions). Indeed, many alerts flagged up by intrusion detection systems (IDSs) are 'false positives'. This is especially if the IDS uses significant deviations from a 'normal baseline' of behaviour as a basis for issuing an alert ('anomaly-based' detection).

As a result, it is difficult for a blockchain administrator to determine whether a real danger actually exists.

Conversely, in the physical asset context, it is easier to tell whether an actual danger exists – for example it is relatively easy to tell whether a building is actually beginning to catch

---

<sup>145</sup> E.g. the block time (time taken to generate a new block) for Ethereum is around 12 seconds.

fire as opposed to whether it is merely producing smoke. The visual cues and tangible evidence provide fewer ambiguities, which allow for a more straightforward risk assessment. Also, the initial signs of danger in the physical asset context typically allow for a longer response time – for example a fire might smoulder for a few minutes before becoming a full blaze.

As a result, blockchain administrators need more leeway in exercising killswitches, relative to the necessity defence threshold for physical assets<sup>146</sup> (which requires actual danger). If administrators need to be sure there is an actual danger, this would often be too late as this means they would not act in the case where there is a reasonable suspicion of danger (e.g. via an alert flagged up by the IDS), because they would not know whether the danger is real or not. If the danger is real, millions of dollars of assets could be taken in seconds.

In other words, the difficulty in distinguishing legitimate blockchain conduct from the initial sign of a hack or bug means that there can be many ‘false positives’, yet at the same time there is a lower tolerance for ‘false negatives’<sup>147</sup> in the digital asset context because of the time-sensitivity and high monetary value of such hacks and bugs. The task of ensuring that false negatives are minimised as much as reasonably possible (i.e. maximising ‘recall’)<sup>148</sup> means that the law needs to have a higher tolerance for administrators exercising killswitches in the case of ‘false positives’, even if that is disruptive to users of the relevant token or blockchain.

Thus, even if we assume that the necessity defence is available in cases of conversion and trespass, it is suggested that the requirement of an ‘actual danger’ would be too harsh on defendants. A defence should be available in certain circumstances despite there being no actual danger to a digital asset, for example where (1) the defendant reasonably suspects that the (actual or likely) harm arising from a suspected bug or hack is significant and imminent, and

---

<sup>146</sup> Assuming the necessity defence is applicable in the first place.

<sup>147</sup> I.e. where there is a danger, but that is missed by the intrusion detection system.

<sup>148</sup> ‘Recall’ is the percentage of actual positive instances that have been correctly identified by the system. Maximising ‘recall’ usually comes at the expense of ‘precision’ (the probability that an instance identified by the system as positive corresponds with an actual positive).

(2) the defendant's conduct in exercising the killswitch is a reasonable and proportionate response to the suspected bug or hack.<sup>149</sup>

Overall, it is clear that the threshold of 'fair warning' and the relevant contextual considerations are very different across physical and digital assets, which means one would expect a substantially different scope of liability in respect of interferences with the latter.

### **3.5 Argument 2: Chattel tort rules themselves are unsatisfactory and arguably too harsh**

The law surrounding chattel torts is unsatisfactory. The rules themselves are messy and needlessly complex, in that they are shrouded in unnecessary conceptual baggage and vague language. Also, the strict liability of the chattel torts is arguably too harsh as it gives rise to problems for innocent defendants. Therefore, applying the same rules to digital assets would lead to the same undesirable features being replicated in the digital asset context.

Three features will be explored: (1) the 'right to immediate possession' concept, (2) the lack of a universal definition of conversion and vague formulations of the tort, and (3) the strict liability nature of the chattel torts.

#### ***3.5.1 'Right to immediate possession'***

The 'right to immediate possession' concept is highly problematic, and should not be applied in the digital asset context.<sup>150</sup> It is used to determine the outer limits of whether a person has title to sue in conversion,<sup>151</sup> but the language of 'right to immediate possession' is

---

<sup>149</sup> These ideas are based on the necessity defence, and one could also consider the further condition that the circumstances in (1) were not created by the defendant's own negligence (see Virgo (n 139 above), 156.

<sup>150</sup> For more discussion of this point, see Chapter 2, Section 3.2.1.2 above; Hin Liu, 'Title, control and possession in the digital asset world' [2022] LMCLQ 597, 611-612.

<sup>151</sup> A person can sue in conversion if they have actual possession or the right to immediate possession.

fundamentally vague and does not provide much guidance. It is unhelpful insofar as ‘right to immediate possession’ is synonymous with ‘right to sue for interference with possession’, and it is also unhelpful insofar as a person with title to the goods already has a right to possess the goods.<sup>152</sup> In this sense, the notion of a ‘right to immediate possession’ does not provide much further guidance on what is required to have title to sue for conversion. It does not easily map onto the threshold of ‘you must have title,<sup>153</sup> but not have granted a chattel lease or pledge’, and many judges have made mistakes (e.g. in holding that a mere contractual right to possession confers title to sue).<sup>154</sup>

This vague language of ‘right to immediate possession’ is problematic because it obscures the issue of whether the chattel lease is a derivative interest, as well as the *numerus clausus* debate that informs it.<sup>155</sup> These issues are fundamental and need to be clarified, because the general principle across property law is that a person with title can sue for interference unless he has granted a derivative interest. Yet, these considerations are not confronted in the conversion context, and are hidden under the concept of the ‘right to immediate possession’. At the same time, the technical language gives it the appearance of legitimacy despite it merely being a conclusory label: a ‘right to immediate possession’ describes the default rights of a person who has title (insofar as he has a right to exclude), but is vague and unhelpful as a *test* for who has the right to sue for interference. This gives judges room to reach a desired conclusion without transparent reasoning to justify it.<sup>156</sup>

If the ‘right to immediate possession’ concept were to be applied in the digital asset context, this conceptual confusion (as well as room for opaque reasoning) will be replicated,

---

<sup>152</sup> See Liu (n 150 above), 611.

<sup>153</sup> This includes relative titles.

<sup>154</sup> As noted by Curwen: see Nicholas Curwen, ‘Title to sue in conversion’ (2004) Conv 308, 312-316.

<sup>155</sup> The *numerus clausus* debate is engaged because the issue arises as to whether the chattel lease is on the permitted list of property rights under English law, and if not, whether the reasons in favour of recognising it on the list of property rights outweighs the reasons against: see e.g. Liu, ‘Title, control and possession’ (n 150 above), 611. See also Ben McFarlane, ‘Identifying property rights: a reply to Mr Watt’ (2003) Conv 473, 486-487.

<sup>156</sup> See discussion at Chapter 2, Section 3.2.1.2 above.

and the fundamental *numerus clausus* and ‘fragmentation of title’<sup>157</sup> issues will not be clarified let alone confronted.

### 3.5.2 Definitions and formulations of conversion

Also, there is no universal definition of conversion, and the current formulations of conversion are vague. Indeed, Lord Nicholls in *Kuwait Airways*<sup>158</sup> stated that it is “well nigh impossible” to define the tort,<sup>159</sup> and Selvam J also noted that conversion is “too elusive to be expressed in words”.<sup>160</sup>

The lack of a clear formulation of the tort makes it difficult for people to know the normative threshold for interference, insofar as it requires them to slice through a layer of conceptual baggage to discern what the general normative threshold is.

For example, conversion has been referred to as a denial of the claimant’s title to the chattel<sup>161</sup> by a defendant’s assertion of title over the claimant’s chattel.<sup>162</sup> This formulation does not provide much practical guidance, as it raises the questions of (1) what acts constitute a *denial* of title, and (2) what acts constitute an *assertion* of title by the defendant. Similarly, conversion has been described as an “intentional act or dealing with goods” that is “inconsistent with or repugnant to the rights of the owner”.<sup>163</sup> This again does not provide much practical

---

<sup>157</sup> This issue arises because the chattel lessor is not allowed to sue, yet the chattel lease does not contain the features of a proprietary interest. See e.g. Simon Douglas, *Liability for Wrongful Interferences with Chattels* (Hart Publishing, 2011), 33-36 (chattel lease does not contain the features of a proprietary interest).

<sup>158</sup> *Kuwait Airways* (n 74 above).

<sup>159</sup> *ibid*, [39]. Lord Nicholls states that “framing a precise definition of universal application is well nigh impossible”.

<sup>160</sup> *The Endurance I* [2000] SGHC 99, [30]. Likewise, Prosser has noted that some of the definitions of conversion have been “so general and so vague in their terms as to be meaningless”: William L Prosser, ‘Nature of Conversion’ (1957) 42 Cornell L Rev 168, 168.

<sup>161</sup> Bridge et al (n 78 above), 33-014 (and fn115).

<sup>162</sup> *Ibid*, 33-014; *Hollins v Fowler* (1872) LR 7 HL 757, 785: “acts done with the intention of transferring or interfering with the title to or ownership of [goods], or which are done as acts of ownership of them”; *Lancashire and Yorkshire Railway Co v MacNicol* (1918) 88 LJKB. 601, 605: “an intention on the part of the defendant ... to deny the owner’s right or to assert a right which is inconsistent with the owner’s right”.

<sup>163</sup> *Bunnings Group Ltd v CHEP Australia Ltd* [2011] NSWCA 342, [124].

guidance, because it raises the question of when the act becomes ‘inconsistent with’ or ‘repugnant to’ the rights of the owner.<sup>164</sup> It is far from clear that formulations like ‘denial and assertion of title’ or ‘inconsistency’ or ‘repugnancy’ map on to the substantive threshold for conversion set out in Section 3.3 above.<sup>165</sup>

Such formulations, if interpreted at face value, can produce many different results. It is difficult to infer the general threshold for interference from such formulations/definitions, and it is necessary therefore to slice through a layer of conceptual baggage in order to discern the general threshold. This causes confusion and uncertainty: indeed, the authors of *The Law of Personal Property* note that “much of the difficulty in conversion lies in estimating the required seriousness of the defendant’s interference”,<sup>166</sup> and similarly Douglas notes that it is an “almost impossible task for a lawyer to advise a client on the merits of a possible claim”<sup>167</sup> outside certain well-established categories of conversion. These problems will be replicated in the digital asset context, as judges will not be able to discern with ease what the threshold requirement for interference is, and may reach arbitrary decisions because of the lack of guidance provided by the existing formulations of conversion.

Also, the fundamental purpose of vagueness is to provide the necessary flexibility to respond to context, to avoid running the risk of making the formulation overly precise (which causes over-inclusiveness and under-inclusiveness).<sup>168</sup> However, the vagueness that exists in the chattel torts goes beyond what is necessary to respond to context. One can be a lot more precise than this, for example by adopting a formulation of conversion that makes it reasonably

---

<sup>164</sup> Indeed Allsop P in *Bunnings* (n 163 above) (at [124]) also quoted Lord Nicholls’s statement in *Kuwait Airways* (n 74 above) that the tort is “well nigh impossible” to precisely define.

<sup>165</sup> See Section 3.3 above, in particular Section 3.3.1.

<sup>166</sup> Bridge et al (n 78 above), 33-014.

<sup>167</sup> Douglas (n 74 above), 198.

<sup>168</sup> See e.g. Timothy Endicott, ‘Law is Necessarily Vague’ (2001) 7 *Legal Theory* 379; Timothy Endicott, *Vagueness in Law* (OUP, 2008).

clear what is required: Douglas for example suggests conversion should be defined as “an intentional exercise of exclusive control” over another’s chattel”.<sup>169</sup>

### 3.5.3 *Strict liability*

Furthermore, the strict liability nature of the chattel torts is arguably too harsh on innocent defendants, as it holds them liable for honest but reasonable mistakes.<sup>170</sup> For example, if an asset is sent to the defendant, and he sends it to someone else under the (honest and reasonable) mistaken belief that he owns the asset, he commits conversion and is liable to pay the full value of the goods to the defendant.<sup>171</sup> This can be seen as an unfair result, because it often defeats reasonable expectations of the defendant, given that there are many situations where such a defendant may very reasonably believe that he owns the relevant goods.<sup>172</sup> Also, it becomes very hard for people to plan their activities in such a way that they can predict the legal consequences of those activities, and they would either (1) need to expend time and cost to verify whether the asset is owned by someone else (in order to avoid the risk of liability), and often never find out the answer, or (2) simply refrain from acting (or attempt to avoid getting

---

<sup>169</sup> See Douglas (n 74 above), 199. This yields significantly more determinate results than formulations such as ‘denial’ and ‘assertion’ of title, or intentional acts that are ‘inconsistent’ with or ‘repugnant’ to the rights of the owner, which are either circular or insufficiently helpful. Such formulations are vague and do not act as a sufficient constraint on the outcomes that can be reached by a judge in a particular case. For example, the notion of whether the defendant’s action is ‘repugnant’ to the rights of the owner is a matter of subjective judgement, and gives rise to a very wide possible range of interpretations and thus outcomes that can be reached in a particular case. This stands in contrast with Douglas’ proposed formulation, because the idea of an intentional exercise of ‘exclusive [physical] control’ is relatively clear in English law (such as in the adverse possession context: see e.g. *Powell v McFarlane* (1977) 38 P & CR 452, 470-471, *J A Pye (Oxford) Ltd v Graham* [2002] UKHL 30, [2003] 1 AC 419, [40]-[41]) and is much less subjective, thus significantly constraining the possible outcomes that can be reached by a judge.

<sup>170</sup> Nick Curwen, ‘The remedy in conversion: confusing property and obligation’ (2006) 26 LS 570, 582-583; SFC Milsom, *Historical Foundations of the Common Law* (2<sup>nd</sup> ed, Butterworths 1981) 379; Norman Palmer and Ewan McKendrick (eds), *Interests in Goods* (2<sup>nd</sup> ed, London: LLP Profession Publishing 1998) ch 32.

<sup>171</sup> He is also liable if he mistakenly believes he is authorised to do so. Milsom provides the example of an “innocent auctioneer [who] sells another’s property”: see Milsom (n 170 above), 379. See also *Willis v British Car Auctions* [1978] 1 WLR 438, 442 (auctioneer liability for sale and subsequent delivery to purchaser).

<sup>172</sup> Or that there is no one with a superior right, or that his action(s) are authorised. A defendant is liable no matter how bona fide his belief that there is no adverse interest or that his action(s) are authorised: see e.g. *OBG* (n 19 above), [311].

themselves into situations where goods may be owned by a third party). Insofar as this result is thought to be unfair,<sup>173</sup> it should not be replicated in the digital asset context.<sup>174</sup>

For example, a centralised digital asset exchange could receive a cryptocurrency from a client (especially if it has done the relevant AML/KYC<sup>175</sup> checks) into its own address where the client did not have the ‘best’ title.<sup>176</sup> In this case, the exchange would receive the client’s (inferior) title,<sup>177</sup> and either hold it on trust, or hold it outright subject to a contractual obligation to return an equivalent quantity of cryptocurrency.<sup>178</sup> If the exchange later uses the cryptocurrency for proprietary trading, and executes an on-chain transfer of the cryptocurrency to its counterparty (without knowing of the defect in title),<sup>179</sup> this would prima facie constitute a conversion in the absence of a bona fide purchase defence,<sup>180</sup> and the ‘true’ owner<sup>181</sup> could bring an action against the exchange. This can be seen as an undesirable result as it causes problems for innocent exchanges: they may end up being liable in conversion, and thus take defensive measures to avoid this risk, even if such measures cause a wasteful depletion (or otherwise inefficient use) of their assets.<sup>182</sup>

---

<sup>173</sup> For general arguments that strict liability is unfair or has the potential to be unfair, see e.g. Ernest Weinrib, *The Idea of Private Law* (OUP, 2012), ch 7; Thomas Nagel, *Mortal Questions* (CUP, 2012) 31; HLA Hart, *The Concept of Law*, (2<sup>nd</sup> ed, OUP 1994), 173 and 178-9. Also, the Law Commission note that the strict liability nature of conversion means that there may be “unjustified...liability in tort [in the digital asset context]” should conversion be extended to digital assets, for example in situations where “participants will interact with digital objects – largely by taking control of them – without knowing any information about their counterparty”: see Law Commission, *Final Report* (n 66 above), 9.73.

<sup>174</sup> Also, where the relevant action from the defendant does not involve a *purchase* (e.g. where a defendant freezes or burns (or executes an on-chain transfer of) a digital asset he believes he owns), a bona fide purchase defence would not operate to avail him even if such a defence were to exist. Thus, even with a bona fide purchase defence, having strict liability would not offer sufficient protection to defendants insofar as such a regime would still hold them liable for honest but reasonable mistakes.

<sup>175</sup> Anti-money laundering (AML) and know your customer (KYC).

<sup>176</sup> I.e. where he had an inferior relative legal title.

<sup>177</sup> There is currently no bona fide purchase defence for digital assets.

<sup>178</sup> Hin Liu, Louise Gullifer and Henry Chong, ‘Client-intermediary relations in the crypto-asset world’ in Paul Davies and Tan Cheng-Han, *Intermediaries in Commercial Law* (Hart Publishing, 2022), 213.

<sup>179</sup> I.e. where the exchange does not know that it does not have the best title.

<sup>180</sup> Nonetheless, although there is currently no bona fide purchase defence for digital assets, the Law Commission are suggesting that there should be a bona fide purchaser rule that applies to all crypto-assets (see Law Commission, *Consultation Paper* (n 44 above), 13.84, and 13.50-13.90). It remains uncertain whether this change would be implemented.

<sup>181</sup> I.e. the person with the best title.

<sup>182</sup> See also City of London Law Society, *Law Commission Consultation Paper on Digital Assets – Response of the City of London Law Society* (4<sup>th</sup> November 2022), 17.

### 3.6. Argument 3: Combinative effect – mistakes by judges

We have established that (1) the differences in digital and physical assets mean that the normative threshold of the chattel torts cannot be directly applied to digital assets (and causes uncertainty and/or incorrect results), and (2) the chattel tort rules are unsatisfactory and cause problems for innocent defendants, in which case applying them into the digital asset context leads to the replication of the same errors.

It is suggested that when (1) and (2) are combined, this creates a very substantial risk of seven types of mistakes being made by judges (some of which have already been mentioned briefly).<sup>183</sup> First, normatively irrelevant features of an asset/environment can be mistakenly considered as relevant. Second, normatively relevant features of an asset/environment can be mistaken as irrelevant. Third, normatively irrelevant features of a rule can be taken as relevant. Fourth, a rule can be applied directly to a new context with the effect that the wrong normative result can be reached. Fifth, doctrine can be intentionally ‘bent’ or ‘stretched’<sup>184</sup> such that the wrong normative result is reached.<sup>185</sup> Sixth, judges may make bare assertions or reason opaquely, especially when vague concepts are used. Seventh, the judge may end up opening the door to disrupting the *physical* asset threshold.

Of course, these mistakes can be made by judges in any context. However, in this particular context, the risk of these mistakes is substantially higher because (1) blockchain

---

<sup>183</sup> See Section 3.2, para 5, and Section 3.4, paras 7-8 (last two paras) above.

<sup>184</sup> ‘Bending’ or ‘stretching’ a doctrine involves applying a doctrine in a way that is incompatible with its normative rationale.

<sup>185</sup> Here, the normative result would be wrong in that there would be too much or too little liability on defendants overall, but the judge considers the outcome to be the desired normative result *on the facts* (e.g. because he is sympathetic with the claimant’s circumstances). An example would be the contractual ‘right to immediate possession’ situation (see Section 3.6.2 below).

technology is relatively unfamiliar to judges,<sup>186</sup> and (2) the rules on chattel torts are unsatisfactory and apt to mislead.

Three examples will be given to illustrate the range of mistakes that can be made by a judge.

### ***3.6.1 Consent and necessity***

The first example (which has been explored previously)<sup>187</sup> is the application of the ‘consent’ and ‘necessity’ defences to digital asset interferences that involve the use of a killswitch or burn/freeze permission being exercised in response to a (reasonably) suspected bug or hack. Where the claimant has not consented to (e.g.) his digital asset being frozen,<sup>188</sup> the defendant would not have any defence if the chattel tort rules were extended (and applied) to this situation.

However, there is a strong argument that this creates the wrong normative result (mistake 4) for the reasons mentioned earlier in Section 3.4.2 relating to the different policy balance in the blockchain environment. For example, killswitches might be needed to prevent or stop the effect of suspected hacks or bugs that may threaten the integrity or fundamental operation of the relevant blockchain or significantly affect the use of (or access to) assets within such a blockchain, and blockchain administrators need to act swiftly instead of wait until there is an actual danger.

This is because (*inter alia*) it is difficult to distinguish between legitimate conduct and the initial signs of a hack or bug, many people can be affected at once by hacks and bugs, a large amount of high value assets can be quickly misappropriated or drained, further damage could be done to the blockchain and internal company operations, and limiting the (potential

---

<sup>186</sup> As compared to physical assets.

<sup>187</sup> See Section 3.4.2 above.

<sup>188</sup> And assuming that the particular act of freezing constitutes an actionable interference.

or actual) damage from these hacks and bugs is a time-sensitive task. Thus, on this argument, a defence should be available despite the absence of consent from the claimant and there being no actual danger to a digital asset, in circumstances where (for example) the two conditions of the suggested defence in Section 3.4.2 above ((1) reasonable suspicion of imminent and significant harm from a suspected bug or hack, and (2) reasonable and proportionate response) are satisfied.<sup>189</sup>

Alternatively, a judge who wants to offer a defence may stretch the notion of consent to include ‘logic consent’<sup>190</sup> on the basis that the claimant opted into the environment (mistake 5), and support this conclusion based on ‘code is law’ literature.<sup>191</sup> However, ‘logic consent’ is not actual (express or implied) consent, because there is no consent to the *interference*. It is difficult to draw an analogy with the signature rule in contract (where people are bound by the relevant contract by virtue of their signature despite not reading the fine print), because at least in that situation the terms are in natural language (which affords people a reasonable opportunity to read and understand the terms). Conversely, with code, the average blockchain user would not be reasonably expected to be able to read the underlying code or understand it: there would simply be no fair warning.<sup>192</sup>

Stretching the notion of ‘consent’ may also carry knock-on effects on the physical asset threshold (mistake 7). This is because a defendant may attempt to rely on a defence where he has interfered with a physical asset in circumstances where the claimant has not consented to the interference but in some way ‘opted in’ to an environment under the defendant’s control (and use ‘digital asset logic consent’ to bolster its conclusion, by showing that actual consent is not necessary for a defence to apply, and that opting into an environment may be taken as

---

<sup>189</sup> See Section 3.4.2, para 15 (penultimate para) above.

<sup>190</sup> See Section 3.4.2 above.

<sup>191</sup> ‘Code is law’ is a school of thought to the effect that people’s legal rights are governed by the code itself: see e.g. Lawrence Lessig, *Code: And Other Laws of Cyberspace, Version 2.0* (Basic Books, 2006), 5, 77.

<sup>192</sup> It may be difficult to discern the meaning of natural language terms that are obscure or in ‘fine print’, but discerning the meaning of code is orders of magnitude more difficult for the average blockchain user.

sufficient). If this argument succeeds, the defences threshold in the chattel torts would be disrupted.<sup>193</sup> Even if this argument does not succeed, it would be a waste of time and resources because judges would still need to deal with the argument and go through much more material in the process.

### ***3.6.2 'Right to immediate possession' in the context of a blockchain token***

While physical assets are familiar to judges (as objects they interact with on a day-to-day basis), digital assets are substantially less familiar to judges. This increases the risk of inadvertent mistakes.

Mistakes can arise in the context of determining whether someone has a 'right to immediate possession' (for the purpose of title to sue in conversion), by emphasising irrelevant features of the rule and of the asset. Suppose that C has the best property right to (and controls in his address) a token (X) which confers a contractual right to another token Y, contained in an exchange's smart contract address. Y is redeemed by way of sending X into the smart contract address (with the process being fully automated). If Y is stolen by a thief (D), the question is whether C has title to sue D. A judge may be tempted to confer a right to sue, and may as a result focus on the fact that the token redemption process under the smart contract is 'immediate' (in that the process of redemption happens instantaneously in an automated

---

<sup>193</sup> Because the 'consent' defence would go beyond actual (express or implied) consent. It is a core tenet of property law that property rights should be protected against non-consensual interferences. As such, any 'consent' defence should only exist where there is actual consent to the interference, because only then would the claimant's autonomy (his choice of whether to permit the defendant's interference) be sufficiently respected. Therefore, if there is no actual (express or implied) consent, the default position is that there should not be a 'consent' defence. If there is another reason why the defendant ought not to be liable, this could be reflected in the form of another defence. Allowing a 'logic consent' argument (i.e. 'C opted into my environment, and it does not matter that he did not actually consent') to succeed would decrease the protection of property rights, without careful debate or justification for doing so. Doing so goes beyond the rationale of the consent defence under the chattel torts, and such an argument should not be allowed to succeed through the back door via an expansive interpretation of a word that is made possible as a result of such word being interpreted (inappropriately) expansively in another context.

fashion), thereby deciding that C has a right to ‘immediate’ possession. This ignores two features. First, the notion of ‘immediate’ possession in the context of the title to sue rule has no normative significance apart from distinguishing between reversionary interests and immediate interests,<sup>194</sup> meaning that the automation and immediacy of execution of smart contracts is irrelevant to the normative threshold of the rule (mistake 3).<sup>195</sup> Second, having the best property right to X merely confers a *contractual* right to the token Y, and contractual rights to possession (or their digital ‘equivalent’)<sup>196</sup> do not allow a claimant to sue in conversion.<sup>197</sup> Yet it is easy to ignore this feature because of the automated and fast-paced nature of the digital asset environment (mistake 2).<sup>198</sup>

A judge’s temptation to confer a right to sue may result from the fact that (for example) the exchange is unwilling to sue to recover the asset, such that the only means of recourse would come from the claimant directly suing the defendant. This sympathy for the claimant could lead to doctrine being bent in a way that generates the wrong result (mistake 5).<sup>199</sup> Also,

---

<sup>194</sup> Reversionary and immediate *proprietary* interests.

<sup>195</sup> The notion of ‘immediate’ possession is used to distinguish between two *legal* concepts or features, namely (1) reversionary interests, and (2) immediate interests: there would be a right to sue if the claimant has an immediate interest but not if he has a reversionary interest. The automation and immediacy of execution of smart contracts is a *factual* feature of the technology, instead of a *legal* feature. This feature is completely independent of whether the claimant has a reversionary interest or an immediate interest. Thus, it is irrelevant to whether there is a right to ‘immediate’ possession for the purpose of the title to sue rule.

<sup>196</sup> A contractual right to obtain exclusive control of token Y.

<sup>197</sup> A proprietary right is required: *Jarvis v Williams* [1955] 1 WLR 71; Curwen (n 154 above), 309, 314-316; *Bridge et al* (n 78 above), 33-039; *Jones et al* (n 23 above), 16-62.

<sup>198</sup> This mistake has been made by judges in the physical asset context (see e.g. nn 200-201 below and text thereto in relation to *Dutton*). In the digital asset context there is a higher risk of such a mistake being made, given that judges are less familiar with digital assets as compared to physical assets.

<sup>199</sup> The effect of a contract between C and X (including the contractual right here in respect of token Y) on a stranger (D)’s duties are carefully policed by the economic torts, as made clear by Lord Hoffmann in *OBG* (n 19 above) at [99] (see also Douglas and McFarlane (n 106 above), 238-239). These torts impose fault-based liability. As such, if C is conferred a right to sue in conversion based on a mere contractual right, this would be the wrong result because it would impose strict liability for interference with contracts, and undermine the carefully policed limits of the economic torts. Indeed, Curwen notes that a contractual right to possession should not give rise to a right to sue in conversion because doing so would mean “strict liability would replace fault-based liability”: see Curwen (n 154 above), 316.

Introducing strict liability in commercial dealings is undesirable because it is very difficult to discover whether someone has a contractual right to immediate possession (see Curwen (n 154 above), 316-317; see also Douglas and McFarlane (n 106 above), 239).

Indeed, the orthodox view requires that the claimant have a legal property right before he can sue in conversion: see n 197 above. There are comments to the contrary in *Government of the Islamic Republic of Iran v Barakat Galleries Ltd* [2007] EWCA Civ 1374, [2009] QB 22, at [26] and [30] but they are *obiter* and inconsistent with the orthodox view.

as mentioned in Section 3.5.1 above, the ‘right to immediate possession’ concept is vague and creates the risk of opaque reasoning that appears to be legitimate because of the technical doctrinal label. This scenario gives room for judges to be able to reason opaquely (e.g. in relation to ‘immediate’) so as to reach the desired result on the facts.

We also see these mistakes in the physical asset context where distinctions are conflated. For example, in *Manchester Airport v Dutton*,<sup>200</sup> the Court of Appeal majority held that the claimant licensee who never took possession of the relevant piece of land had the right to possession against the defendants (who were protesters occupying the land without permission), and so the claimant was able to obtain a possession order against the defendants. This was despite the fact that the claimant had no proprietary interest in the land: (1) the claimant had a contractual licence instead of a lease and thus did not have a derivative property interest from the owner, and (2) the claimant did not take possession of the land and thus did not have an original relative title. Thus, without a proprietary interest, the claimant should not have had the right to sue.<sup>201</sup> Similarly, the ‘equivalent’ mistake in the digital asset context (in the ‘right to immediate possession’ example) would be the judge conflating a contractual right to (immediate) ‘possession’ or ‘control’ of token Y (which is enforceable against the contractual counterparty) and a proprietary right to token Y that is enforceable against the world. The former does not suffice because there is no proprietary right and thus no right to exclude.<sup>202</sup> In

---

<sup>200</sup> [2000] QB 133. For more examples, see Section 3.6.3 below (in relation to the *OBG* and *Shell* cases).

<sup>201</sup> The *numerus clausus*, which provides for a closed list of (legal) property rights enforceable against the world at large (see e.g. Law of Property Act 1925, s.1), functions to limit the circumstances under which a person can acquire a right that is good against the world (and thereby limit the duties of third parties such that their liberty is not unduly stifled). Such a right can only be acquired if one has a property right on the closed list.

A mere contractual licence like the one in *Dutton* is not a property right on the closed list, and thus should not create a right to exclusive possession that is good against the world (including the defendant stranger). This is noted by Swadling, who notes that the decision in *Dutton* violates the *numerus clausus*: see William Swadling, ‘Opening the numerus clausus’ (2000) 116 LQR 354, 354, 358-359.

Also as in n 199 above, imposing strict duties on the defendant (here to relinquish possession) violates the carefully policed limits of the economic torts in relation to the liability of D for interfering with a contract between C and X. Furthermore, as noted by Swadling (n 201 above) at 358-359), allowing the claimant in *Dutton* to enforce his contractual right against a third party stranger violates the privity principle in contract law, whereby a right to a contract is only enforceable against his counterparty.

<sup>202</sup> See nn 197 and 199 above, and Curwen (n 154 above).

addition, the majority in *Dutton* may have been motivated by a desire to confer a right to sue on the claimants because of the political sensitivity and potential reputational harm that could have been caused by the National Trust (the owners of the land) suing the defendants (hence stretching doctrine to reach a just result on the facts). Similarly, a judge may be motivated to confer a right to sue on the owner of token X because the exchange refuses to sue.

This scenario also clearly demonstrates that the mistakes noted above are caused by a combination of (1) physical and digital assets being different in nature and behaviour, and having different surrounding environments, and (2) the rules on conversion being unsatisfactory. For example, the mistake relating to ‘immediate’ possession arises from the fact that (1) the ‘immediacy of execution’ feature unique to smart contracts/digital assets was treated as more relevant than the underlying contractual arrangements between the parties, thus mistaking noise for signal, and (2) the ‘right to immediate possession’ concept (with its misleading language of ‘immediate’ and its obscure normative basis) is what enables judges to mistakenly emphasise the wrong features of digital assets when reaching a *conclusion in the context of the title to sue rule*.

### **3.6.3 Frozen token**

Where a blockchain token is frozen by the defendant (such that the claimant is unable to transfer the token out of his address), the judge may use an analogy from the physical asset space to determine whether the tort of conversion (or trespass) has been committed.

In *Burroughes v Bayne*,<sup>203</sup> the tort of conversion was committed in respect of the claimant’s billiards table when the defendant locked the door to the room in which the table

---

<sup>203</sup> *Burroughes* (n 76 above).

was located. If the frozen (or ‘locked’)<sup>204</sup> digital asset is a ticket to a service, or an NFT, a judge may use the *Burroughes* analogy and vary it so that the relevant physical object is a physical ticket or a piece of physical artwork (in which case there would still be a conversion of the physical asset). The judge may then reason by analogy that locking a service token or an NFT would also constitute conversion.<sup>205</sup>

This seems like an intuitively good analogy but on closer inspection it is unsatisfactory insofar as the asset may contain transactional functionalities apart from the power to transfer. First, it draws a false parallel with physical assets because it emphasises a feature of physical assets that is irrelevant/inapplicable to digital assets (mistake 1). With a physical asset, locking it in a room where you do not have the key to it means that it cannot be used at all.<sup>206</sup> If your physical concert ticket is locked in a room in which you do not have the key, your use of the ticket is completely impaired. You cannot physically move it at all, and a ticket needs to be physically presented at the venue before it can be used for admission. On the other hand, a digital asset that allows someone to access a service (e.g. a concert) via a blockchain transaction can still be used to access that service despite being frozen in its address.

Indeed, it ignores a relevant feature of digital assets (mistake 2): they can still be used for other blockchain transactions despite being frozen in an address. A digital asset that is frozen in its address may still (if programmed in such manner) be used to gain access to concerts or exclusive events by signing a blockchain transaction.<sup>207</sup> Similarly, certain digital assets can contain transactional powers to vote or bid, or take in-game actions (such as changing their avatar to the picture in their NFT), or claim an airdrop reward.

---

<sup>204</sup> In the context of a digital asset, the terms ‘frozen’ and ‘locked’ are often used interchangeably.

<sup>205</sup> If locking a room that contains a billiards table is conversion, locking a room that contains physical artwork or a physical ticket would also be conversion. In *Shin v ICON Foundation* (Case No. 20-cv-07363-WHO (N.D. Cal. May. 11, 2021)), the claimant made this argument in a ‘frozen token’ case, arguing that the analogy is with a landlord who locked the door to the house in which the claimant tenant’s personal property is contained: see p.16).

<sup>206</sup> Indeed, Douglas characterises *Burroughes* as a ‘complete impairment of use’ case: Douglas (n 76 above), 96.

<sup>207</sup> One can still sign a signature from the address in which the digital asset is contained, using the private key to the address.

Indeed, digital assets can be used despite an inability to be ‘moved’ between addresses because the digital environment is different from the physical environment. In contrast, a physical asset can in general only be used if one can make physical contact with it.

The combinative effect of these two mistakes (mistakes 1 and 2) is that conversion or trespass may now be committed without a ‘physical interference’ (or its equivalent) even in *partial* interference cases. There was no physical contact or damage in *Burroughes*, and if it is used as an analogy, then this would disrupt the threshold for the chattel torts since the ‘physical interference’ requirement would effectively be removed.<sup>208</sup>

Yet, the analogy between a locked/frozen token and *Burroughes* can be easy to make because of the terminology of ‘locked’ or ‘frozen’, and a locked token can be seen in many ways as similar to a physical asset locked in a room (since the asset is effectively ‘immobilised’ within the ‘space’ of the public address of the asset). Also, even if the asset is eventually ‘unlocked’ in *Burroughes*, there would still be conversion, and this parallels the situation where a digital asset is eventually ‘unlocked’ by the defendant. It is easy to skip over the ‘physical contact/damage’ requirement under the chattel torts because this is a requirement inferred from the case law instead of expressly stated.

This creates knock-on effects in the physical asset context (mistake 7). A claimant who has a physical asset that is partially (as opposed to completely) impaired as a result of the defendant’s conduct may make an argument that there is a conversion or trespass even if there is no physical contact or damage. He can rely on the ‘frozen token’ scenario to bolster his case, and with (*ex hypothesi*) the amount of potential noise in the case law on digital assets, a judge may be swayed into granting such a claim.<sup>209</sup> If such a claim is granted, the outcome would be

---

<sup>208</sup> And this would be inconsistent with *Club Cruise* (n 85 above).

<sup>209</sup> Even if the argument does not succeed, the judge would still need to spend time dealing with the argument, which would not be an efficient use of time as he would have to go through and consider much more material. See also Liu, ‘Title, control and possession’ (n 150 above), 615.

inconsistent with *Club Cruise*<sup>210</sup> (where there was no liability under the chattel torts because of a lack of physical contact or damage in relation to the ship).

Another mistake that may be made in the ‘frozen token’ case is that a judge may assert that the situation involves the ‘broad equivalent’ of physical contact or damage (by using an analogy such as ‘locking the asset into a safe’), without justifying its choice of analogy (another example of mistake 1). This mistake can be easy to make since one may feel that (for example) the ‘locking into a safe’ analogy is intuitive and does not need to be justified with rigorous reasoning. Yet the similarities and differences need to be compared in detail in order to avoid false analogies.<sup>211</sup> Without a detailed comparison of the differences, this makes the reasoning opaque (mistake 6), and makes it difficult for people to know what the real threshold for ‘equivalence’ is.

The mistake of making ‘intuitive’ analogies without considering the differences in detail, which results in the wrong conclusion being reached, can be seen throughout property law. For example, in *Shell v Total*,<sup>212</sup> the defendant carelessly damaged land that was held on trust for the claimant, and it was held that the claimant (as trust beneficiary) had the right to sue a defendant in negligence, on the basis that the claimant was ‘in substance’ the owner of the asset.<sup>213</sup>

Essentially, the Court of Appeal drew the ‘intuitive’ analogy between the claimant’s position and that of legal owner (who would have the right to sue for negligence),<sup>214</sup> and held that they were similar enough such that the claimant had the right to sue. However, this conflates the fundamental difference between someone who has title and someone who is a beneficiary under a trust: only the former has the right to possession of the asset and thus the

---

<sup>210</sup> *Club Cruise* (n 85 above).

<sup>211</sup> Such as the false analogy with *Burroughes*.

<sup>212</sup> *Shell UK Ltd v Total UK Ltd* [2010] EWCA Civ 180.

<sup>213</sup> *ibid*, [143]: “it would be a triumph of form over substance to deny a remedy to the beneficial owner...when the legal owner is a bare trustee for that beneficial owner”.

<sup>214</sup> *Leigh & Sullivan Ltd v Aliakmon Shipping Co Ltd (The Aliakmon)* [1986] AC 785.

right to sue for interference (in this case for negligence). A trust beneficiary simply does not have a right to possession of the asset and thus does not have the right to sue.<sup>215</sup> As such, the Court of Appeal reached the incorrect conclusion in holding that the claimant had the right to sue.<sup>216</sup>

The same mistake can be seen in Baroness Hale's minority speech in *OBG*, where she held that choses in action should be amenable to a claim in conversion. She held that (1) since conversion protects (personal) property, and (2) choses in action (just like physical goods) are personal property, (3) choses in action should be amenable to a claim in conversion.<sup>217</sup> Although she makes the 'intuitive' analogy between physical assets and choses in action insofar as are both valuable and transferable assets, she ignores the core feature of physical assets: that they are tangible and have discernible boundaries, such that the ways in which one can interfere with a physical asset are relatively circumscribed and one has a reasonable degree of fair warning. In contrast, the content of a chose in action can be tailored and selected by the parties, meaning that there are many potential ways for a defendant to interfere with a chose in action.<sup>218</sup> Imposing strict liability for interferences with choses in action would therefore be

---

<sup>215</sup> *Shell* is not consistent with previous authorities, which deny that a stranger owes a duty to a trust beneficiary not to interfere with the property that is the subject of the trust. See e.g. *Earl of Worcester v Finch* (1600) 2 And 162; *Lord Compton's Case* (1580) 3 Leo 197; *The Aliakmon* (n 214 above); *MCC Proceeds v Lehman Brothers International (Europe)* [1997] EWCA Civ 3068, [1998] 4 All ER 676. This is noted by Douglas and McFarlane: Douglas and McFarlane (n 106 above), 241-242. See also Sinead Agnew and Ben McFarlane, 'The Nature of Trusts and the Conflict of Laws' (2021) 137 LQR 405, 416, where the authors note that the "orthodox position" is that the beneficiary has no claim against the defendant. Conflating the distinction between legal title and a trust beneficiary's interest would impose extra burdens on defendants without their consent and without their conscience being affected by notice or knowledge of the equitable interests (Douglas and McFarlane (n 106 above), 242. This undermines the fundamental principle that equitable interests are not enforceable against third parties whose conscience is not affected by notice or knowledge of the interest (see e.g. *Akers v Samba Financial Group* [2017] UKSC 6, AC 424, [89]; *Investec Trust (Guernsey) Ltd v Glenalla Properties Ltd* [2018] UKPC 7, [2019] AC 271, [228]; Ben McFarlane and Simon Douglas, 'Property, Analogy and Variety' (2022) 42 OJLS 161, 179-180.

<sup>216</sup> Indeed, *Shell* has been widely criticised: see e.g. James Edelman, 'Two fundamental questions for the law of trusts' (2013) 129 LQR 66; PG Turner, 'Consequential economic loss and the trust beneficiary' (2010) 69 CLJ 445; Emma Hargreaves, 'The nature of beneficiaries' rights under trusts' (2011) 25 TLI 163, 165-166; Douglas and McFarlane (n 106 above), 242-243; McFarlane and Douglas (n 215 above), 179-180.

<sup>217</sup> *OBG* (n 19 above), [308]-[310].

<sup>218</sup> E.g. if C lends £20 to X where X has one year to repay the debt, but X does not have to repay the debt if Lionel Messi scores more than 20 goals this season, C cannot sue Lionel Messi (D) for 'interfering' with his right to repayment if Messi scores 25 goals this season (insofar as Messi has 'extinguished' his right to the £20 and thus 'interfered' with his right to repayment).

overly harsh on defendants. It would also circumvent the existing restrictions on recovery of pure economic loss<sup>219</sup> under the economic torts (which generally require a high mental element),<sup>220</sup> and in negligence (which requires a failure to take reasonable care and an assumption of responsibility).

### **3.6.4 ‘Digital trespass and conversion’ cases in other jurisdictions**

At this point, one may nonetheless argue that the existence of ‘intangible trespass and conversion’ cases in other jurisdictions means that extending the chattel torts to digital assets does not pose a problem. It is argued that this conclusion is mistaken, for two reasons.

First, most of the cases involving conversion and trespass to intangible assets do not involve an interference with digital assets: they mainly involve impairments of use of digital files or domain names.<sup>221</sup> It does not follow that digital assets should be covered by conversion and trespass.<sup>222</sup> There are policies specific to the digital asset environment that are not relevant in the context of digital files or domain names, such as the composability of the underlying blockchain environment. This leads to the wrong normative threshold being applied to digital assets, for example where (as mentioned earlier)<sup>223</sup> the ‘consent’ defence in conversion and trespass does not take into account the fact that a defendant blockchain administrator ought to be able to impair use of a claimant’s digital assets in some situations where he needs to engage a killswitch and freeze the state of the blockchain in order to prevent a suspected bug or hack.

---

<sup>219</sup> Curwen (n 116 above), 316-317.

<sup>220</sup> For example, inducing breach of contract requires knowledge that the course of conduct would amount to a breach of contract, plus an intention to procure such a breach: See Jones et al (n 23 above), 23-32 – 23-38. Causing loss by unlawful means requires an intention to cause loss to the claimant: Jones et al (n 23 above), 23-81.

<sup>221</sup> As well as spam cases: see e.g. *CompuServe* (n 63 above).

<sup>222</sup> And reversionary injury.

<sup>223</sup> See Sections 3.4.2 and 3.6.1 above.

In any event, some of the conversion cases involving intangible assets can be recharacterised. For example, where the claim involves impairment of use of a domain name (e.g. where the defendant fraudulently persuades the domain name registrar to register a domain name in his favour), this is in essence a claim for pure economic loss. A domain name involves a contractual right against the service provider, and a domain name by itself confers no title to any separate object of property (such as the underlying computer servers that perform the relevant operations in respect of the domain name). Here, there would be a remedy under the unlawful means tort.<sup>224</sup> It is suggested that since there is no interference with any concrete object of property to which the claimant has title or a ‘possessory’ interest,<sup>225</sup> domain name interferences should not by themselves<sup>226</sup> fall within the scope of the property torts.

Second, although there are US cases that have applied the chattel torts to digital assets,<sup>227</sup> this does not change the fact that the three core arguments in this article still apply as far as English law is concerned. The fact that the chattel torts apply to digital assets in the US does not remove the fact that the cases often involve complex factual scenarios that require nuanced balancing acts (where the English chattel torts are unsuited to dealing with). An example would be *Shin v ICON*,<sup>228</sup> where an unintended loophole in the code caused the claimant to mint extra tokens for free. The defendant administrators of the blockchain system froze the claimant’s tokens without his consent.<sup>229</sup> The system rules enabled such freezing to

---

<sup>224</sup> There would be deceit against X (the domain name registrar): there has been a fraudulent representation to the domain name registrar, which the registrar has acted upon. Even if the registrar suffers no loss as a result of the deceit, the ‘wrong to third party’ element is satisfied: *OBG* (n 19 above), [49].

<sup>225</sup> The terminology of a ‘possessory’ interest is ambiguous, but I am referring to an inferior relative title or a derivative interest such as a pledge. Also, the Law Commission has noted that domain names are not data objects because there are not independent of the legal system: see Law Commission, *Consultation paper* (n 44 above), 8.19 and 8.24.

<sup>226</sup> I.e. in the absence of damage to any physical object.

<sup>227</sup> See e.g. *Williams v Mahmood* (Case No. 6:21-cv-03074-RK); *Archer v Coinbase Inc* 53 Cal App 5th 266, 267 Cal Rptr 3d 510 (Cal Ct App 2020); *Kleiman v Wright* Case No. 18-CV-80176-BLOOM/Reinhart (SD Fla Dec 27, 2018); *Shin* (n 205 above).

<sup>228</sup> *Shin* (n 205 above).

<sup>229</sup> And compelled Binance and Kraken to freeze the tokens that were transferred to them. Given limitations of space (and for the purposes of simplicity) I will focus on the tokens frozen directly by ICON.

occur, and the act of freezing was intended to reverse the effects of the loophole/bug in the code.

The conversion issue was not fully dealt with in the judgment given the nature of the application,<sup>230</sup> but a judge who is tasked with tackling the issue in full would need to deal with a complex and nuanced balancing act. One needs to balance (1) the fact that the defendant impaired the use of the claimant's digital asset, and (2) the fact that the claimant minted extra tokens in accordance with the rules of the system/program, against (3) the defendant's desire to reverse the unintended effects of the program.

If we were to apply the English law chattel torts to the facts of *Shin*, we would again run into the risk of the physical asset threshold producing the wrong normative result in the digital asset context. Assuming there is a relevant interference (based on the fact that there was a complete impairment of use of the claimant's digital assets), the 'consent' defence would not be available to the defendant since the claimant did not consent to the freezing of the tokens. However, the 'consent' defence does not take into account the fact that it may be justified for the defendant to exercise a killswitch especially in situations where there was an unintended loophole/bug in the code that was exploited by the claimant. Also, the necessity defence (if it applies to the chattel torts) is not made out here because there is no actual danger to existing assets, but merely an increase in the supply of new assets (via the minting of tokens).

Ultimately, after balancing the relevant considerations, a judge may reach the conclusion that from a normative perspective there should not be a defence, but the problem is that there is simply no doctrinal tool to even take the relevant sides of the issue into account.

---

<sup>230</sup> See e.g. *Shin* (n 205 above), p15-18 (conversion issue dealt with briefly). The case involved a motion to strike.

Having no defence *to consider* apart from consent<sup>231</sup> means that this crucial issue does not even end up being discussed.<sup>232</sup>

#### 4. Option 2: A new regime

It is suggested that formulating a new regime that deals specifically with digital asset interferences, and allows people who have a property right to a digital asset to recover control of it, would be preferable to extending the chattel torts to digital assets.

This regime has two components:

- (1) an impairment tort that deals with situations where the claimant's ability to use his digital asset has been intentionally or recklessly impaired; and
- (2) a 'recovery of control' remedy that entitles the claimant to recover control of a digital asset (without establishing liability in tort) where:
  - (a) he has a property right; and
  - (b) the defendant is in control and has either a worse property right or no property right.

---

<sup>231</sup> Statutory defences are not relevant in this situation.

<sup>232</sup> Also, if we were to slightly vary the facts of *Shin*, we can see the potential for more messy reasoning. Suppose for example that the token owned by the claimant contained many functionalities such as voting and dividend rights. If the defendant administrator had disabled some rights but not all, causing a partial (instead of a total) impairment of use) this would run into the problems raised earlier (in Section 3.6.3) in relation to the 'frozen token' example, such as the use of intuitive physical analogies that may not be the most accurate.

Indeed, physical analogies were made in the judgment (e.g. the claimant drew the analogy between his situation and a "slot machine that continued to provide jackpot winning each time he put quarters in and pressed the same buttons" (p5), as well as a "tenant whose landlord has locked him out of his apartment and denied him access to personal property inside").

This regime creates a good normative balance between the need to protect claimants (property right holders) and the need to preserve the liberty of potential defendants. It produces much better outcomes than extending the chattel torts to digital assets, as it avoids many of the problems associated with doing the latter, and reflects the core aim of conferring a property right to a digital asset. The regime should also be introduced through legislation instead of common law development.

The two components of the proposed regime will be explored in turn, followed by a discussion of why the regime is superior to extending the chattel torts to digital assets, and why change should be implemented through legislation instead of case law development.

#### **4.1 Impairment tort**

The impairment tort is the primary mechanism to address wrongs committed by defendants in respect of digital asset(s) to which the claimant has a property right, in situations where the defendant has a worse property right or no property right. The core idea behind this tort is that the claimant in such situations would be entitled to bring an action where the defendant has impaired the claimant's ability to use his digital asset(s), either intentionally,<sup>233</sup> or recklessly.<sup>234</sup>

The conduct and mental elements of the tort will be explored in turn.

##### ***4.1.1 The conduct element***

It is suggested that the conduct element of the impairment tort should be organised around the notion of impairing someone's (present or future) ability to use a digital asset (an "impairment

---

<sup>233</sup> As defined in Section 4.1.2 below.

<sup>234</sup> As defined in Section 4.1.2 below.

of use”).<sup>235</sup> As the core purpose of non-interference rights in the digital asset context is to protect a right-holder’s ability to use their digital asset,<sup>236</sup> the impairment tort should give effect to this purpose.<sup>237</sup>

As such, if someone’s ability to use his digital asset has been impaired, the general position is that there should be a remedy (provided other conditions such as a particular mental state, and causation between the defendant’s act and the relevant impairment, are satisfied).

In the digital asset context, what does it mean for a defendant to have *impaired* the use of the claimant’s asset?<sup>238</sup> It is suggested that there is an impairment if there is prejudice or detriment to someone’s ability to exercise the functionalities associated with the digital asset. Paradigm cases of impairment would include the ‘core’ cases of misappropriating, burning, or freezing a digital asset, in situations where the claimant knows the private key. In these cases, the claimant’s ability to use the asset is totally prevented or significantly diminished, for either a specific period or forever.

Also, if the defendant makes a transaction on the blockchain in respect of the claimant’s asset in a way that deprives the claimant of the opportunity of making the same transaction (e.g. using the claimant’s private key to exercise a vote in relation to the claimant’s digital asset),<sup>239</sup> that would also be an impairment of use. The defendant’s action has prevented the claimant from exercising a power that he had. Furthermore, disabling certain functionalities that someone can exercise in respect of a digital asset using his private key, such as the power to vote on certain transactions, would also constitute an impairment of use.

---

<sup>235</sup> Douglas uses the two terms ((1) impairment of use and (2) impairment of ability to use (and/or words to that effect)) interchangeably: see Douglas (n 76 above), 93-96 (conversion and trespass) and 101 (negligence). I will use the two terms (and words to that effect) interchangeably as well.

<sup>236</sup> I.e. his ability to exercise the transactional powers associated with the digital asset.

<sup>237</sup> See Chapter 1, Section 6.3.1 above.

<sup>238</sup> An asset to which claimant has a property right, and where the defendant does not have a better property right.

<sup>239</sup> Where that vote cannot be revoked, and the claimant knows the private key.

Denying the claimant access to his digital asset via a DDoS attack (on e.g. the mobile application or website used by the claimant to access his digital asset, the blockchain network nodes, or the API that connects the front-end application used by the claimant and the blockchain back end architecture) would also constitute an impairment of use. This is because the DDoS attack prevents the claimant from being able to exercise the functionalities associated with the digital asset using his private key.

There are other ways of denying access to a digital asset that constitute an impairment of use, but which also involve committing one of the chattel torts. For example, this can happen in the context of a USB device where the private key is contained and sealed. If the defendant steals the USB device, the claimant would be unable to access his digital asset. The same would be the case if the defendant steals the computer in which the private key is contained (and the contents of the data on that computer have not been backed up).

This would constitute (1) an impairment of use of a digital asset, as well as (2) conversion. Nonetheless, in these situations, most claimants would prefer to sue the defendant in conversion because there is no need to prove the mental elements of intention or recklessness in respect of the impairment tort (explored below).<sup>240</sup>

The outer boundaries of what constitutes an ‘impairment’ for the purpose of the impairment tort is an open question. For example, would a relatively slight effect on use count as ‘impairment’ of use of a digital asset, in situations where (e.g.) the defendant slows down the website that the claimant uses to access his digital asset? Would this constitute ‘detriment’ or ‘prejudice’ to the claimant’s ability to exercise the functionalities associated with the digital asset?

The answer would depend on one’s view on how far the claimant should be protected, and how far the defendant’s liberty should be preserved. This is an open question, but there is

---

<sup>240</sup> See Section 4.1.2 below.

a strong argument for construing ‘impairment’ relatively widely given that the proposed mental requirement is relatively high (intention or recklessness)<sup>241</sup> and acts as a significant constraint on liability.

It is suggested that leaving what constitutes an ‘impairment’ open to interpretation by the courts, instead of rigidly defining it, will allow the courts to develop jurisprudence that is sensitive to contextual nuances. This is especially the case in areas involving emerging technologies such as blockchain where a degree of in-built flexibility will allow the courts to respond appropriately to situations that cannot be foreseen in advance.<sup>242</sup>

Importantly, impairment of use does not encompass the ‘mere interference with usability’ situations raised in Chapter 1 position 5, where there can be liability in nuisance even though the claimant’s factual ability to exercise the uses in relation to the property (land) has not been impaired.

The example raised in Chapter 1<sup>243</sup> in relation to ‘mere interference with usability’ was where D emits fumes with disproportionately foul odours on C’s land for 12 hours when C is halfway across the world and is travelling for two months. There is liability in nuisance in this situation even though C’s use of his land has not been impaired (given he would not in any case have used his land in that 12 hour period). There is an ‘interference with usability’ (and thus liability) because the land itself is not capable of being used and enjoyed to the same extent – a hypothetical person who is on C’s land in that 12 hour period would have his use and enjoyment of the land affected by the odours.

A rough equivalent of this situation in the digital asset context would be if D intentionally freezes an asset to which C has a property right, where at that time C has

---

<sup>241</sup> Explored in Section 4.1.2 below.

<sup>242</sup> Yet, the focus on ‘impairment’ will allow the courts to be clear on what the general threshold is, instead of having them grapple with the uncertainty of what ‘proxy’ for physical interference should be adopted in the digital asset context.

<sup>243</sup> At Chapter 1, Section 6.2.2.5 above.

misplaced his private key, and D unfreezes the asset before C finds his private key. Here, there is no impairment of use because C's factual ability to exercise the transactional abilities associated with the digital asset has not been diminished. As he has misplaced his private key, he could not have exercised the abilities in that time period when the asset was frozen. Nonetheless, there is an 'interference with usability' because a hypothetical person with the private key would not have been able to enter blockchain transactions in respect of the asset in that time period as a result of the freeze, when he otherwise would have been able to.

It is suggested that this situation should not give rise to liability because there has been no impairment of C's ability to use his digital asset. Conversely, if he had not misplaced his private key during that time period, then there would have been liability since his ability to exercise the transactional functionalities in respect of the digital asset would have been impaired, given that he could not have exercised the transactional functionalities that were disabled by the freeze (e.g. transfer, voting).

What if D intentionally burns C's digital asset (or freezes it without subsequently unfreezing it), where at that time C has lost his private key, but he later recovers it? It is suggested that C can sue from the moment he recovers the private key, because that is the moment where but-for the burn/freeze, he would have had the factual ability to make transactions on the blockchain using the private key.<sup>244</sup> There is an impairment of use from that point onward because it is from that time that his ability to exercise the functionalities associated with the digital asset has been prejudiced.

The above analysis also illustrates a key distinction in relation between positions 4 and 5 explored in Chapter 1 – position 4 requires there to be an *actual* impairment of use whereas position 5 does not. This could be an actual impairment of one's present ability to use, or an actual impairment of one's future ability to use.

---

<sup>244</sup> And there is no issue of remoteness.

Support for the ‘impairment of use’ approach can be found in the DIFC DAL, which adopts it as the organising concept in Article 14.

The primary conduct element of Article 14 is that the defendant “impairs the use of the Digital Asset to which [the claimant] is entitled” (Article 14(2)(b)). As stated in the DAL Consultation Paper, the rationale of having ‘impairment of use’ as an organising concept is to protect the claimant’s use of the digital asset and thus directly give effect to the purpose of the right to exclude.<sup>245</sup>

Nonetheless, Article 14 requires the claimant to establish loss before he can sue for impairment, and one may wonder whether loss should be a necessary condition for a claimant to sue.

It is suggested that loss should not be a necessary condition for liability under the proposed impairment tort. Loss is not a necessary condition of liability in many torts (such as trespass),<sup>246</sup> and where there is no loss, there can be an award of nominal damages to demonstrate that the right has been violated. It is suggested that the same should be the case in the context of the impairment tort. Where the defendant impairs the use of a digital asset to which the claimant has a property right,<sup>247</sup> and suffers loss, he should be awarded substantial damages in respect of his losses, but even if he does not suffer loss (e.g. if the claimant would not have used the asset during the period of the impairment),<sup>248</sup> the fact remains that the claimant’s ability to use the asset has been impaired. Nominal damages should be awarded to vindicate the right that has been interfered with.<sup>249</sup>

---

<sup>245</sup> DIFC, *Consultation Paper* (n 70 above), paras 86, 88, 89.

<sup>246</sup> *Transco Plc v United Water Utilities Plc* [2005] EWHC 2784 (QB) at [22]; *William Leitch and Co Ltd v Leydon* [1931] AC 90, 106; *Bridge et al* (n 78 above), 33-003; *Jones et al* (n 23 above), 16-02 and 16-141.

<sup>247</sup> Provided that there is a particular mental element, explored immediately below (from the next paragraph onwards).

<sup>248</sup> Such as where C’s digital asset is frozen and subsequently unfrozen by D, and C has the private key to the digital asset, but C would not have exercised any blockchain transactions during the period of the freeze.

<sup>249</sup> Nominal damages are valuable to the claimant for various reasons: see e.g. Sadie Blanchard, ‘Nominal Damages as Vindication’ (2022) 30 *Geo Mason L Rev* 227, 251-8.

#### *4.1.2 The mental element*

As for the mental element, it is suggested that the threshold should be satisfied by intention or recklessness. In other words, there should be liability if the defendant:

- (1) intends the impairment of use of digital asset(s), while he does not believe he has the best property right to the asset(s) or that all person(s) with a superior property right<sup>250</sup> have authorised the impairment ('intention'); or
- (2) is aware of a real risk that the use of digital asset(s) to which he has no property right or does not have the best property right will be impaired, does not believe he has the best (or any) property right to it, does not believe all person(s) with a superior property right have authorised the impairment, and unreasonably takes that risk ('recklessness').

In relation to the intention requirement, it is important to draw a distinction between someone intending the impairment per se, versus intending the impairment without believing that (1) he has the best property right to the digital asset, or that (2) people with a superior property right have consented to the impairment. If intending the impairment per se were enough for liability, this would essentially be a strict liability standard like that applied in the chattel torts – the chattel torts also have a requirement that the relevant act is an intentional act.<sup>251</sup> Thus, the 'belief' caveat functions to protect the defendant from liability in situations where he honestly but mistakenly believes that he has the best property right to the digital asset, or that all person(s) with a superior property right have consented to the impairment.

---

<sup>250</sup> This includes the situation where the defendant does not have a property right (in which case all person(s) with a property right would have a superior property right).

<sup>251</sup> See e.g. *Bridge et al* (n 78 above), 33-006 (trespass) and 33-015 (conversion; "intentional assertion of title").

The 'belief' caveat also exists in relation to the recklessness requirement, for the same reason. It would prevent defendants from being liable where they honestly believe they have the best property right to the relevant digital asset, or where they honestly believe all person(s) with a superior property right have consented to the impairment.

It is suggested that the recklessness standard (i.e. recklessness or intention as defined above), as a starting point, provides a reasonable balance between the interests of claimants and defendants.

Requiring an intention to impair the use of the claimant's digital asset would be undesirable, this would result in too little liability for defendants. For example, if a person calls a function on the blockchain and foresees that there is a significant risk of someone else's digital assets being damaged or destroyed, and unreasonably takes such a risk, the fact that he did not intend the damage or destruction should not absolve him of liability.

This person would satisfy the 'recklessness' standard of liability, and it is suggested that the recklessness standard strikes a reasonable balance between the claimant's interest in not having the use of his digital asset impaired and the freedom of action of potential defendants.

This is because the recklessness standard prohibits actions that involve a conscious decision to put one's own interests above those of others, by deliberately disregarding the latter in an unreasonable way. This is readily established in relation to intention (as defined above), but recklessness (as defined above) also involves a conscious disregard of the risk that the use of someone else's digital asset would be impaired, coupled with the taking of an unreasonable risk.<sup>252</sup> In the tangible property context, recklessness is also the mens rea requirement for the 'Destroying or damaging property' offences under s.1(1) and 1(2) of the Criminal Damage Act 1971.<sup>253</sup>

---

<sup>252</sup> See also e.g. Marcia Baron, 'Negligence, mens rea, and what we want the element of mens rea to provide' (2020) 14 Criminal Law and Philosophy 69, 71-73 (discussion of recklessness as "conscious disregard" of risk).

<sup>253</sup> Criminal Damage Act 1971, s.1(1); *R v G* [2004] 1 AC 1034.

The recklessness standard also encourages people not to take unreasonable risks that they are aware of (in relation to impairing the use of a digital asset). This unreasonable risk-taking can happen on the blockchain. For example, D could call a function on the blockchain knowing there is a real risk it has a bug or feature that (if activated via a function call) has a significant probability of causing damage to digital assets. If the taking of such risk is unreasonable, a recklessness standard (which would impose liability in such situations) would discourage this kind of unreasonable risk taking.

Indeed, the two requirements of (1) subjective foresight of a risk on the part of the defendant, and (2) ‘unreasonably’ taking the risk that the defendant foresees, provides crucial constraints on liability.

The mental requirement suggested here (intention or recklessness) is also adopted in Article 14 of the DIFC DAL.<sup>254</sup>

#### 4.1.2.1 A lower threshold?

Should there be a lower threshold, such as negligence? It is suggested that imposing a negligence threshold would also be undesirable as it imposes too much liability on defendants.

For example, in the context of developer liability, blockchain developers generally know that if they are careless in writing code, there is a risk that the use of digital assets can be impaired.<sup>255</sup>

This would disincentivise people from developing programs on the blockchain. Such a result would be undesirable, as it would discourage innovations in the blockchain space, and run counter to the open-source ethos of the blockchain and crypto space.<sup>256</sup>

---

<sup>254</sup> DAL, Articles 14(1) and 14(2)(c).

<sup>255</sup> There may be contractual disclaimers of responsibility but general baseline standard still applies.

<sup>256</sup> In an open-source environment, people have access to each other’s code. People can build programs that are based on other people’s code, instead of needing to write the code from the ground up. If open source code is

Imposing a negligence standard in this context would be more analogous to imposing general negligence liability for pure economic loss, as opposed to negligence liability for damage to a physical asset. Like with pure economic loss, there are many ways of causing damage to a digital asset (given that a digital asset can be programmed in so many ways, including being programmed in a way such that it is burnt or frozen when certain conditions are satisfied).

For example, a digital asset can be programmed in a way where its existence<sup>257</sup> depends on the price of an asset being above or below a certain level as reported by a website or series of websites.<sup>258</sup> If these website(s) negligently misreport the price data in a way that destroys or (burns) the digital asset in a way where it would not have been destroyed (or burned) but-for the misreporting,<sup>259</sup> they should not be held liable.<sup>260</sup> Website operators would be exposed to potentially indeterminate liability in circumstances where it is extremely difficult to gather information about which digital assets would be damaged or destroyed by their negligent conduct.

This contrasts with a physical asset, which is generally only damaged if one is in physical proximity to it. Also, if one is in physical proximity to a physical asset, one generally only needs to make a minor and intuitive adjustment in order to avoid damaging it (such as walking around it).

It is therefore relatively easy to avoid damage to a physical asset, and as such, a general negligence threshold can be adopted in relation to physical assets, where one can be liable for

---

used by many parties and the bugs are replicated in a lot of subsequent code, the potential economic losses can be enormous if people can be sued for negligence.

<sup>257</sup> Or functional existence (i.e. its existence in a non-burn address).

<sup>258</sup> E.g. in the derivatives context. Suppose that C buys a digital asset for a certain price via a smart contract, where the conditions stipulate that the asset is burnt the price of a stock (X) goes below £30 (as reported by certain website(s)), but C benefits from the upside if X is at £50 or above.

<sup>259</sup> E.g. (using the same example) if the website(s) negligently misreport the price of X as being £25 when it is in fact above 30, the token is burnt. If the (real) price of X does not drop below 30, and later goes to 80, C would suffer a loss of £30.

<sup>260</sup> And *a fortiori* where the digital asset is frozen and would not have been frozen but-for the misreporting.

negligently causing damage to a physical asset provided that the damage is reasonably foreseeable.<sup>261</sup>

In contrast, the fact that economic loss is much more easily caused, and much harder to avoid, means that there are extra safeguards in place for careless defendants who cause pure economic loss.<sup>262</sup> People cannot foresee the extent of the economic losses they cause or the parties to which they may be liable, and this makes it very difficult for parties to know that they have not caused pure economic losses.

Because of these reasons, the law imposes a higher threshold of liability for negligently caused economic losses: in general, an assumption of responsibility is required.<sup>263</sup> If economic loss that is caused by carelessness or negligence *per se* leads to liability, this would unduly stifle the liberty of defendants and potentially create a hypervigilant society.<sup>264</sup>

Similarly, there should not be liability for negligently causing the impairment of use of digital assets. Just like with pure economic loss, is difficult to know or foresee what digital assets may be damaged as a result of one's negligent conduct,<sup>265</sup> and one may be exposed to indeterminate liability.

#### ***4.1.3 Superior and inferior property rights***

Where the defendant has satisfied the conduct and mental elements of the impairment tort the question arises as to who can sue the defendant under the impairment tort.

---

<sup>261</sup> By virtue of the neighbour principle in *Donoghue v Stevenson* [1932] AC 562, and the normal operation of causation and remoteness rules in tort. See also Goudkamp and Nolan (n 21 above), 5-014.

<sup>262</sup> See e.g. discussion at Goudkamp and Nolan (n 21 above), 5-049.

<sup>263</sup> *ibid*, 5-049; and see cases cited at n 35 above.

<sup>264</sup> Also see discussion by Edelman J in *Mallonland Pty Ltd v Advanta Seeds Pty Ltd* [2024] HCA 25.

<sup>265</sup> A digital asset can be programmed to be destroyed under any condition, and the condition could correspond with D's negligent conduct, such as carelessly causing the price of an asset to be misreported on a website.

If the claimant has a property right to the digital asset, the general position is that he can sue for interference. He can sue a defendant who does not have a property right to the asset, as well as a defendant who has a property right to the asset that is inferior to that of the claimant's. However (and to state the obvious), he cannot sue a defendant who has a property right that is superior to that of the claimant, because of the doctrine of relative title.<sup>266</sup> This position is also reflected in Article 14 of the DAL.<sup>267</sup>

This thesis does not explore the question of what 'lesser interests' can exist in respect of digital assets (such as e.g. the equivalent of a pledge), and therefore does not deal with the question of whether a 'lesser interest holder' has title to sue.<sup>268</sup> Undoubtedly however, these are crucial issues to be explored in future research.

#### **4.2 'Recovery of control' remedy**

Nonetheless, the impairment tort does not protect the claimant in all deserving situations. In situations where C has a property right to a digital asset but has no control of it, and X has control (without having a property right superior to C's), C should be able to recover control of the digital asset even where X has neither intentionally nor recklessly impaired the use of the digital asset.<sup>269</sup> This is necessary to protect C's ability to use the digital asset.

For example, there could be a bug or malfunction in the code that modifies the address of a particular digital asset that was originally in C's address (and to which C has the best property right), such that it is now in X's address (without C's consent). C needs a remedy to recover control of the digital asset, even if X has no idea about the asset that is in his address.

---

<sup>266</sup> Which, as established in Chapter 2, should also apply to digital assets.

<sup>267</sup> DAL, Article 14(1).

<sup>268</sup> It also does not deal with the impact of the creation of such an interest on the grantor's ability to sue (ie 'reversionary injury' in respect of digital assets).

<sup>269</sup> Such that the impairment tort is not constituted.

Thus, a remedy is needed whereby the claimant with a property right to a digital asset can recover control of it if the defendant has control and (1) does not have a property right, or (2) has a worse (inferior) property right. If these conditions are satisfied, the ‘recovery of control’ remedy should be available.

The ‘recovery of control’ remedy reflects the core purpose of having non-interference rights, as it protects the claimant’s ability to use his asset by allowing him to recover control of it.<sup>270</sup>

Article 15 of the DIFC DAL also provides this mechanism. A claimant with legal title can recover control of a digital asset if it is “in the control of another person or group of persons” (Article 15(1)(a)), and “[the defendant] has no legal title to the Digital Asset or has a legal title that is inferior to [that of the claimant]” (Article 15(1)(b)).

Also, insofar as a ‘right to exclusive control’ (Position 2 under Chapter 1)<sup>271</sup> provides remedies in the situation that a person is deprived of control of his asset, the ‘recovery of control’ remedy gives effect to such a right.

As mentioned earlier,<sup>272</sup> this thesis does not look at lesser interests in digital assets. It will therefore will not cover the equivalent of situations involving a ‘term bailment’ (insofar as they may involve lesser interests). Nonetheless, future research could focus on whether a person in the ‘term bailor’s situation has fragmented his proprietary right, or merely granted a

---

<sup>270</sup> This does so directly than (e.g.) a constructive trust under *Westdeutsche* (n 16 above), for two reasons. First, even though a constructive trust under *Westdeutsche* does allow recovery of control in some situations (e.g. in *Ho* (n 16 above), one needs to satisfy its conditions (fruits of theft or fraud, or unconscionability (knowledge of the facts alleged to affect the defendant’s conscience)). It therefore does not cover the whole territory (e.g. an accidental bug that transfers the asset to someone else (B)’s address without fraud or theft, and without B knowing about the asset. Second, a trust is circuitous way to recover control, as it consists of two steps (i.e. imposing a trust, then recovering the property), as compared to the direct route of recovering the property in one step.

<sup>271</sup> See Chapter 1, Section 6.2.2.2 above (Position 2).

<sup>272</sup> See text to n 268 above.

contractual right to the ‘term bailee’. This may then affect the availability of the ‘recovery of control’ remedy as there may be qualifications to the ability to exercise it.<sup>273</sup>

### **4.3 How this regime is superior to extending the chattel torts to digital assets**

In order to demonstrate that this regime is superior to extending the chattel torts to digital assets, it needs to be shown that this regime yields better outcomes, as compared to extending the chattel torts to digital assets.

To establish this point, I will first explore the ‘recovery of control’ remedy, and then the impairment tort.

#### ***4.3.1 ‘Recovery of control’ remedy***

In terms of the ‘recovery of control’ remedy, it is suggested that this remedy yields superior outcomes to having conversion and/or trespass deal with the equivalent situation. This is because there is no need to (1) be subordinated to a damages claim by default where one then needs to actively persuade the court to exercise its discretion to grant in specie recovery,<sup>274</sup> or (2) establish a wrong, and deal with the uncertainty of what constitutes an interference with digital assets under the chattel torts.

It is relatively uncontroversial that if the defendant has control of a digital asset, and the claimant has a property right that is superior to that of the defendant’s (or has a property right but the defendant does not), then the claimant ought to be able to recover control of the

---

<sup>273</sup> For example, one could explore whether the bailor would be entitled to recover the property from the bailee during the term of the hire (if the bailor has not granted a proprietary interest to the bailee). One could also explore whether the bailee would be entitled to a defence, or instead whether the bailor would be entitled to recover the property but be in breach of contract.

<sup>274</sup> Torts (Interference with Goods) Act 1977, s.3.

digital asset.<sup>275</sup> This is the most direct way of reinstating a property right holder's ability to use a digital asset (namely by ordering the defendant to transfer the asset back to the claimant, with the effect that the claimant can exercise the transactional functionalities associated with the digital asset.

If one has the ability to recover the asset in specie, this gives maximal effect to his property right, as he would have direct control of the asset itself and will thus be able to use it. This stands in contrast with the position under the chattel torts, where the default remedy is damages, and where in specie recovery is discretionary.<sup>276</sup> Damages are merely the monetary substitute of the asset – they do not confer direct control over the asset itself, and thus do not restore someone's ability to use it. This is one reason why the 'recovery of control' remedy provides for better outcomes.<sup>277</sup>

In an ideal world, such a remedy should also exist in respect of physical assets – the use of conversion (with damages as the default remedy) to act as a substitute for a direct claim to recover the property is a much more circuitous and incomplete way of protecting property rights in physical assets.

Also, the 'recovery of control' remedy does not involve the defendant committing a tort, and thus does not depend on wrongdoing. As long as the claimant has a property right to the asset, and the defendant has either no property right or a property right that is inferior to that of the claimant's, he is *prima facie* entitled to recover control of the asset. In contrast, with the chattel torts, they are ultimately *torts*, which depend on the defendant having committed some *wrongdoing* as well, as opposed to just having to prove that the defendant has no property right to the asset or a property right that is inferior to the claimant's. The need to prove wrongdoing,

---

<sup>275</sup> Unless the defendant is in control with the consent of someone who has a title superior to that of the claimant, in which case it is suggested that the defendant would have a defence.

<sup>276</sup> Torts (Interference with Goods) Act 1977, s.3.

<sup>277</sup> Also, although a constructive trust under *Westdeutsche* (n 16 above) provides the ability to recover the asset in specie, one needs to satisfy its conditions (fruits of theft or fraud, or unconscionability): there is no ability to recover the asset as of right if one has a property right that is superior to that of the defendant.

in addition to the uncertainties about the substantive threshold required to constitute an interference, impose extra hurdles and unknowns. This is another reason why the ‘recovery of control’ remedy produces outcomes that are superior to that of extending the chattel torts to digital assets.

### ***4.3.2 Impairment tort***

The next step is to establish that the proposed impairment tort produces superior outcomes to extending the chattel torts to digital assets, in situations where the claimant does not seek to invoke (or only invoke) the ‘recovery of control’ remedy.<sup>278</sup>

#### 4.3.2.1 ‘Prima facie’ liability: the conduct and mental elements

In terms of the conduct element, the proposed impairment tort produces better outcomes. This is because it avoids the situation of judges being fundamentally unclear what the threshold is for interference, as would be the case if the chattel torts were to be applied to digital assets. This is the ‘proxy’ issue discussed earlier,<sup>279</sup> where judges are offered no substantive guidance as to what the threshold for interference is, and there are a wide range of thresholds that can be adopted without much certainty about which threshold is likely to be adopted.

In contrast, the ‘impairment of use’ threshold provides a clear formulation insofar as the judge knows he is looking at whether the *use*<sup>280</sup> of an asset has been sufficiently affected by the defendant’s conduct.

---

<sup>278</sup> A claimant may want to invoke both remedies in situations where (e.g.) the defendant is in control of the digital asset, and has caused extra economic loss by committing the impairment tort.

<sup>279</sup> See Section 3.4.1 above.

<sup>280</sup> Ie ability to use.

Although it may be said that the outer boundaries of the ‘impairment of use’ threshold are unclear, it is at least clear that the threshold *is* ‘impairment of use of a digital asset’. This contrasts with the chattel torts being applied to digital assets, where even the *core* cases cannot be enumerated with any real certainty. In relation to what constitutes impairment of use, the core cases are clear (e.g. burning, freezing, misappropriation).<sup>281</sup> This is not the case with the chattel torts in relation to what constitutes an interference, because the need for an ‘equivalent’ to (or ‘proxy’ for) a physical interference means that certain cases of asset freezing or burning where there is an ‘insufficient equivalent’ to physical contact or damage may not satisfy the conduct element of the relevant chattel tort,<sup>282</sup> despite the use of the asset being significantly impaired.

In addition, the high mental requirement of the proposed impairment tort (intention or recklessness) means there is a good safeguard against too much liability even if the boundary cases of what constitutes ‘impairment of use’ are unclear, and a judge interprets the ‘impairment of use’ threshold in a way that is too claimant-friendly. This safeguard does not exist in respect of the chattel torts, which impose strict liability.

Finally, the ‘impairment of use’ threshold is more aligned with the core aim of having a property right to a digital asset, as compared with the threshold under the chattel torts if they were to be extended to digital assets (the substance of which is unclear as far as digital assets are concerned). The former directly targets the core rationale of a property right (namely to protect ability to use), while the same cannot be said about the latter (not least because of the uncertainty in the substantive threshold).

In terms of the mental element, the proposed ‘intention or recklessness’ threshold avoids many of the problems associated with having strict liability. Most notably, the strict

---

<sup>281</sup> Where the claimant has the private key.

<sup>282</sup> See e.g. Section 3.6.3 above.

liability of the chattel torts causes problems where the defendant is under an honest and reasonable mistaken belief that (1) he owns the relevant asset and/or (2) no one else has title to it and/or (3) all superior title holders have consented to the impairment. The defendant would be liable if he damages or destroys the asset, or otherwise satisfies the conduct element of one of the chattel torts.<sup>283</sup> However, under the proposed impairment tort, he would not be liable if he harbours such mistaken beliefs as those beliefs necessarily mean that he does not satisfy the ‘intention or recklessness’ mental element.<sup>284</sup>

#### 4.3.2.2 Defences

At this point, it is clear that the situations that give rise to prima facie liability under the impairment tort regime produce a better normative balance relative to the situations that give rise to the prima facie liability under the chattel torts if they were to be extended to digital assets. One may be tempted to argue that as a result, the regime is superior to that of the chattel torts being extended to the digital asset context.

However, there is one missing step: it must also be shown that the normative balance is superior *after* considering the available defences. This is because if the new regime adopts defences that are too narrow, it may result in defendants being liable in situations where (1) they should not be, and (2) the chattel torts would have offered a defence.

Nonetheless, this step can be established simply by ‘keeping the defences constant’, and considering the position where the new impairment tort adopts the defences of the chattel torts.

---

<sup>283</sup> See Section 3.3 above.

<sup>284</sup> Also, honest but *unreasonable* mistaken beliefs would not lead to liability.

If the impairment tort adopts the defences of the chattel torts, then situations where there is prima facie liability under both the chattel torts and the proposed impairment tort would result in no liability in either where a defence is applicable. As such, keeping the defences ‘constant’ does not lead to situations where there is more liability under the proposed interference regime where there is prima facie liability under both regimes. Where there is prima facie liability under both, there would also not be any *less* liability under the proposed impairment tort, as the defences are the same.

As such, the proposed impairment tort also produces outcomes that are superior to extending the chattel torts to digital assets.

#### **4.4 Why legislation is better than case law development**

The above analysis has established that adopting a new regime based on (1) an impairment tort based on ‘impairment of use of a digital asset’, and (2) a ‘recovery of control’ remedy, would be superior to extending the chattel torts to digital assets.

At this point, it would be appropriate to briefly discuss why a legislative solution that implements the new regime (i.e. implements (1) and (2)) is preferable to incremental common law development of principles of tortious liability in respect of digital assets. This is the case because the latter has been suggested by the Law Commission.<sup>285</sup>

It is suggested that common law development would lead to too much uncertainty, as one would have to wait for an appropriate dispute to arise before the court, and even then the ratio of the relevant decision may only cover a narrow range of situations.<sup>286</sup> It would take too long for the law to become certain enough, and in the interim period, it is likely that the legal

---

<sup>285</sup> Law Commission, *Final Report* (n 66 above), 9.80-9.83.

<sup>286</sup> E.g. if the case only covers burning, it sheds no light on freezing and lesser interferences and what the boundary or threshold may be in terms of the conduct element of the tort.

position in relation to many ‘core’ situations would remain uncertain such that people cannot properly plan their activities, anticipate liabilities, or predict their legal positions.

In contrast, a legislative solution would cover most of the ground, in that the conduct and mental elements of the tort (and the requirements for the ‘recovery of control’ remedy) would be clear, and so would the defences (once the normative balance and legal formulation are worked out). This creates much more certainty, as there are many more situations in which the legal position is clear.

## 5. Conclusion

This chapter has established that extending the chattel torts is not a viable solution to address the gap in protection in respect of digital assets. Instead, it is suggested that a new legislative regime that contains (1) an impairment tort, which imposes (prima facie) liability where the defendant has intentionally or recklessly impaired the use of a digital asset to which the claimant has a property right,<sup>287</sup> and (2) a remedy which allows someone with a property right in a digital asset to recover control of it.<sup>288</sup>

---

<sup>287</sup> One that is superior to that of the defendant.

<sup>288</sup> Provided that the defendant does not have a superior property right.

## **Conclusion and Future Directions**

This thesis explored four research questions:

1. Whether digital assets are conceptually capable of being the subject-matter of property rights, and if so, whether it is normatively desirable to recognise a property right in digital assets; and
2. The circumstances in which it should be possible to acquire a property right in a digital asset for the first time; and
3. The circumstances in which it should be possible to transfer a property right in a digital asset; and
4. The nature and extent of protection against third parties generally that ought to be offered to a holder of a property right in a digital asset.

This conclusion will summarise the arguments that have been made in response to those questions, and then suggest some potential future directions for research that can build on the basic stance set out in this thesis.

### **1. Summary of arguments**

Chapter 1 established that digital assets are capable of being the subject-matter of a property right (in the sense of a non-interference right enforceable against the world), and that it is normatively desirable for a legal system to recognise such property rights.

Chapter 2 explored the conditions under which an original property right to a digital asset should be acquired. It suggested that such a right should be acquired where someone takes

(factual positive and negative) control of a digital asset and has the intention to do so on his own behalf. The degree of control required is to have the higher of (1) enough keys to be able to execute a blockchain transaction, and (2) enough keys to be able to prevent others from being able to execute a blockchain transaction. In mathematical terms, in a M of N address, a person needs the higher of 'M' and 'N-M+1' keys. This translates into having positive and negative control. It also suggested that from a doctrinal perspective, describing this threshold as 'control' is favourable to describing it as 'possession'.

Chapter 3 discussed the appropriate legal requirements for the transfer of such a right. It suggested that such a right should be transferred only where there is a 'change of control' coupled with an intention to transfer the right. This requirement is preferable to the alternatives of requiring an on-chain transfer (with an intention to transfer the property right), or of allowing title to pass by agreement or by deed. However, the types and degrees of control that are sufficient to satisfy the transfer rule is a policy question with no single right answer, and a three-stage approach (considering the normative balance, then the concrete situations and dimensions of control that should be sufficient to transfer title, then the appropriate formulation) should be adopted when considering what the transfer rule should be.

Finally, Chapter 4 explored the issue of protection in respect of digital assets, i.e. the strength of such a right against third parties generally. It established that, under current English law, there exists a gap in protection in respect of digital assets, where deserving claimants are left without a remedy. It also suggested that the best way to fill this gap is not by extending the existing chattel torts to digital assets, but by formulating a new regime that deals specifically with digital asset interferences. The proposed regime contains two elements: (1) a right to sue a defendant who intentionally or recklessly impairs the use of a digital asset, and (2) a right to recover control of a digital asset from a person with no property right or a worse property right in that asset.

## 2. Further research directions

This thesis has laid the foundation for future research by setting out a basic position in relation to my four research questions. This foundation will be useful in considering the many other property law issues that arise in the digital asset context. The following are just a few examples.

First, there can be a much more in-depth exploration of the powers that can and/or should exist in relation to the non-interference right. One can explore the powers to create a trust and charge – and investigate in depth the normative case for recognising such powers, and the appropriate conditions under which such powers can be exercised. Comparisons can be made with the equivalent powers that exist in relation to title to physical assets or debts.

Second, there can be a more extensive discussion of the detail of the appropriate interference regime in relation to digital assets – particularly in relation to defences and remedies.

Third, there can be an exploration of how property rights (in a broad sense) in respect of digital assets can be extinguished, for example in relation to bona fide purchase, or abandonment.

Fourth, there can be a discussion of whether ‘lesser interests’ can and should exist in relation to digital assets, and (if so) the nature of these interests, and the requirements for their creation, transfer, and destruction. This can happen for example in relation to an interest that is the broad equivalent of a pledge or lease.

Fifth, there can be a detailed study of linked assets. What types of links can exist, and when would a link become effective at law? Are there mechanisms to ensure that the link would not be broken, and if not, are there adequate methods of restoring the relevant link or providing

sufficient remedies? This thesis lays the foundation for such effects to be analysed in the context of e.g. digital securities, blockchain bills of lading, and tokenised assets generally.

All of these property law issues have immediate practical relevance in this three trillion dollar market, where the stakes are immense, and where both institutional and retail players are heavily involved in the space. It is imperative to strike the right balance between providing adequate legal rights and protections, encouraging technological and business innovation, preserving the liberty of potential defendants, and providing enough legal certainty – and this requires having a robust property law regime that has sufficiently good solutions to the issues raised above. Having such a regime is – to borrow Merrill’s words, a *sine qua non*.<sup>1</sup>

Aside from the practical questions, one can also undertake a detailed examination of more theoretical questions such as the extent to which cryptoassets can be reconciled with existing models of property, such as in relation to ‘thingness’ (which one may view as a predominantly physical concept).

There are many more issues that can be explored (whether theoretical or practical), such as whether digital assets should be characterised as a ‘third thing’ or a chose in action, as well as whether (and how) the Financial Collateral Regulations should be amended to accommodate digital assets.

It is hoped that this thesis lays the foundation for these issues to be explored, as it clarifies the fundamentals by providing a set of basic ‘building blocks’ in response to my four research questions. It is also hoped that this thesis takes a significant step towards (1) addressing certain gaps in the existing case law, literature and commentary in relation to digital assets, and (2) redirecting the focus towards the important questions that need to be tackled.

---

<sup>1</sup> Just as Merrill views non-interference rights as a *sine qua non* of property (see Thomas W Merrill, ‘Property and the Right to Exclude’ (1998) 77 Neb L Rev 730, 730), I view having a robust property regime for digital assets as a *sine qua non* for the optimal flourishing of the digital asset industry. This, indeed, will be the last analogy I draw in this thesis – the reader may of course question its aim, substance, or technique.

## Bibliography

'Asia's First Spot Bitcoin and Ether ETFs Debut in Hong Kong', *Hauzen* at <https://hauzen.hk/asias-first-spot-bitcoin-and-ether-etfs-debut-in-hong-kong> (accessed 10<sup>th</sup> September 2024)).

'Bitcoin ETF List', *Vettafi* at <https://etfdb.com/themes/bitcoin-etfs/> (accessed 10<sup>th</sup> September 2024)

'Blockchain for Decentralised Finance (DeFi) | Consensys', *Consensys* at <https://consensys.io/blockchain-use-cases/decentralized-finance> (accessed 12<sup>th</sup> September 2024).

'Borrow & lend on the leading NFT liquidity protocol', *NFTfi* at <https://nftfi.com> (accessed 13<sup>th</sup> January 2025)

'Cryptocurrency Prices, Charts And Market Capitalizations | CoinMarketCap', *CoinMarketCap* at <https://coinmarketcap.com> (accessed 31 December 2024 and 1<sup>st</sup> January 2025).

'Double spend (problem) – Glossary | CSRC', *CSRC* at [https://csrc.nist.gov/glossary/term/double\\_spend\\_problem](https://csrc.nist.gov/glossary/term/double_spend_problem) (accessed 31<sup>st</sup> December 2024)

'Ethereum ETF List', *Vettafi* at <https://etfdb.com/themes/ethereum-etfs/> (accessed 10<sup>th</sup> September 2024)

'Four Industries Where DAOs Thrive: Key Use Cases Explored', *Colony* at <https://blog.colony.io/what-are-dao-real-world-use-cases/> (accessed 12<sup>th</sup> September 2024)

'Institutional Money Is Flowing Back Into Crypto – Here's How Margex Copy Trading Helps You to Approach the Markets', *CryptoSlate* at <https://cryptoslate.com/institutional-money-is-flowing-back-into-crypto-heres-how-margex-copy-trading-helps-you-to-approach-the-markets/> (accessed 10<sup>th</sup> September 2024)

'Introduction to the Best Multisig Wallets', *Bitcoin Magazine* at <https://bitcoinmagazine.com/guides/best-multisig-wallets> (accessed 31<sup>st</sup> May 2024)

'Live Cryptocurrency Charts & Market Data | Coinmarketcap', *Coinmarketcap* at <https://coinmarketcap.com/charts/> (accessed 26<sup>th</sup> December 2024)

'Property (Digital Assets etc) Bill [HL] – Parliamentary Bills – UK Parliament', *UK Parliament* at <https://bills.parliament.uk/bills/3766> (accessed 1<sup>st</sup> January 2025)

'Public Name Tags, Labels & Public Notes', *Etherscan* at <https://info.etherscan.com/public-name-tags-labels-public-notes/> (accessed 31<sup>st</sup> March 2023)

'Semler Scientific Expands Bitcoin Holdings to 2,084 BTC, Boosts ATM Offering to \$150M | SMLR Stock News', *Stocktitan* at <https://www.stocktitan.net/news/SMLR/semler-scientific->

announces-updated-btc-and-atm-activity-purchased-rpsv1ug6g6uj.html (accessed 1<sup>st</sup> January 2025)

'The 29 Most Expensive Sold NFTs in the World | POWER.xyz', *POWER.xyz* at <https://power.xyz/engage/story/most-expensive-nfts/> (accessed 3<sup>rd</sup> January 2025)

'Types of Blockchain – GeeksforGeeks', *GeeksforGeeks* at <https://www.geeksforgeeks.org/types-of-blockchain/> (accessed 1<sup>st</sup> January 2025)

'What is a Block Explorer? BTC Block Explorers, etc. | Gemini', *Gemini* at <https://www.gemini.com/cryptopedia/what-is-a-block-explorer-btc-bch-eth-ltc#section-the-block-explorer-a-window-into-the-blockchain> (accessed 2 April 2023)

Agnew S and McFarlane B, 'The Nature of Trusts and the Conflict of Laws' (2021) 137 LQR 405

Alamsyah A, Kusuma GNW and Ramadhani DP, 'A Review on Decentralised Finance Ecosystems' (2024) 16 Future Internet 76

Andersen D, '21Shares files application for spot Solana ETF', *Cointelegraph* at <https://cointelegraph.com/news/21shares-spot-solana-etf-sec> (accessed 10<sup>th</sup> September 2024)

Baron M, 'Negligence, mens rea, and what we want the element of mens rea to provide' (2020) 14 Criminal Law and Philosophy 69

Battersby G, 'Acquiring Title by Theft' (2002) 65(4) MLR 603

Bentham J, *The Theory of Legislation* (London, 1802)

Blanchard S, 'Nominal Damages as Vindication' (2022) 30 Geo Mason L Rev 227

Bridge M, *Benjamin's Sale of Goods* (11<sup>th</sup> ed, Sweet & Maxwell 2020)  
— and Gullifer L, Low K and McMeel G, *The Law of Personal Property* (3<sup>rd</sup> edition, Sweet and Maxwell 2021)

Brown J and Pawlowski M, 'The Challenge of Identifying Private Property under English Law' (2022) 86 Conv 305

Burrows A (ed), *English Private Law* (3rd ed, OUP 2013)

Chan T, 'The nature of property in cryptoassets' (2023) 43 LS 480  
— and Low KFK, 'DeFi Common Sense: Crypto-backed Lending in *Janesh s/o Rajkumar v Unknown Person ('CHEFPIERRE')*' (2023) 86 MLR 1278  
— and Low KFK, 'Post-Scam Crypto Recovery: Final Clarity or Deceptive Simplicity?' — (2023) 139 LQR 379

City of London Law Society, *Law Commission Consultation Paper on Digital Assets – Response of the City of London Law Society* (4<sup>th</sup> November 2022)

Colicev A, 'How can non-fungible tokens bring value to brands' (2023) 40(1) *Int J Res Mark* 30

Cowen T and Tabarrok A, 'Cryptoeconomics' at <https://marginalrevolution.com/wp-content/uploads/2022/05/Cryptoeconomics-Modern-Principles.pdf> (accessed 12<sup>th</sup> September 2024)

Crawford M, *An Expressive Theory of Possession* (Hart Publishing, 2020)

Cryptopedia Staff, 'NFT Art and Music: Blockchain Music Use Cases', *Gemini* at <https://www.gemini.com/cryptopedia/nft-crypto-blockchain-music-industry> (accessed 12<sup>th</sup> September 2024)

Cryptopedia Staff, 'The DAO: What Was the DAO Hack? | Gemini', *Gemini* at <https://www.gemini.com/cryptopedia/the-dao-hack-makerdao> (accessed 31<sup>st</sup> December 2024)

Cutts T, 'Modern Money Had and Received' (2018) 38 *OJLS* 1  
—— 'Possessable Digital Assets: Response to the Electronic Trade Documents Law Commission Consultation Paper No 254 and Call for Evidence on Digital Assets 2021' (2021) LSE Law Policy Briefing Paper No.47

Curwen N, 'Title to sue in conversion' (2004) *Conv* 308  
—— 'The remedy in conversion: confusing property and obligation' (2006) 26 *LS* 570

Davis J, 'The Crypto-Currency | The New Yorker', *The New Yorker*, <http://www.newyorker.com/magazine/2011/10/10/the-crypto-currency> (accessed 29<sup>th</sup> December 2024)

Demsetz H, 'Toward a Theory of Property Rights' (1967) 57 *Am Econ Rev* 347

Dockray M, 'Why do we need Adverse Possession?' [1985] *Conv* 272

Douglas S, 'The nature of conversion' (2009) 68(1) *CLJ* 198  
—— 'Actionable Interferences in the Chattel Torts: A New Perspective on Economic Loss' in Degeling S, Edelman J and Goudkamp J (eds), *Torts in Commercial Law* (Routledge, 2011) 87  
—— *Liability for Wrongful Interferences with Chattels* (Hart Publishing, 2011), 29  
—— 'The argument for property rights in human body parts: scarcity of resources' (2014) 40 *J Med Ethics* 23  
—— and Goold I, 'Property in Human Biomaterials: A New Methodology' (2016) 75 *CLJ* 478  
—— and McFarlane B, 'Defining Property Rights' in Penner J and Smith H (eds), *Philosophical Foundations of Property Law* (OUP, 2013) 219

Dubai International Financial Centre, *Consultation Paper No. 4 (September 2023) Digital Assets Law* (2023)

Edelman J, 'Two fundamental questions for the law of trusts' (2013) 129 *LQR* 66

Ellickson R, 'Property in Land' (1993) 102 *Yale LJ* 1315

- Elliott M and Varuhas J, *Administrative Law: Text and Materials* (5<sup>th</sup> ed, OUP 2017)
- Endicott T, 'Law is Necessarily Vague' (2001) 7 *Legal Theory* 379  
 ——— *Vagueness in Law* (OUP, 2000)
- Epstein RA, 'Possession as the Root of Title' (1979) 13 *Georgia L Rev* 1221
- Fox D, 'Cryptocurrencies in the Common Law of Property' in S Green, D Fox, *Cryptocurrencies in Public and Private Law* (OUP, 2019)  
 ——— 'Digital assets as transactional power' (2022) 1 *JIBFL* 3
- Gold AS, *The Right of Redress* (OUP, 2020)
- Goldberg J, 'Tort Law's Missing Excuses' in Dyson et al (eds), *Defences in Tort* (Hart Publishing, 2015) 53  
 ——— and Zipursky BC, *Recognizing Wrongs* (Harvard University Press, 2020)
- Goode R, 'What is property?' (2023) 139 *LQR* 1  
 ——— and Gullifer L, *Goode and Gullifer on Legal Problems of Credit and Security*, (6<sup>th</sup> ed, Sweet & Maxwell, 2017)
- Goold I, 'Why Does It Matter How We Regulate the Use of Human Body Parts?' (2014) 40 *J Med Ethics* 3
- Goudkamp J, *Tort Law Defences* (Hart Publishing, 2013)  
 ——— and Nolan D, *Winfield and Jolowicz on Tort* (20<sup>th</sup> ed, Sweet & Maxwell 2020)
- Goymour A, 'Bruton v London & Quadrant Housing Trust [2000]: Relativity of Title, and the Regulation of the 'Proprietary Underworld'', in Douglas S, Hickey R and Waring E (eds), *Landmark Cases in Property Law* (Hart Publishing, 2015), 151
- Gray K and Gray SF, *Elements of Land Law* (5<sup>th</sup> ed, OUP 2009)
- Gregson R, 'Is subrogation a remedy for unjust enrichment?' (2020) 136 *LQR* 481
- Green S, 'Theft and conversion – tangibly different?' (2012) 128 *LQR* 564  
 ——— and Randall J, *The Tort of Conversion* (Hart Publishing, 2009)  
 ——— and Snagg F, 'Intermediated Securities and Distributed Ledger Technology', in Gullifer L and Payne J (eds), *Intermediation and Beyond* (Hart Publishing, 2019) 337
- Gullifer L, 'The private law of digital assets: what is it and what should it be?' 2021 Birkenhead Lecture, Gray's Inn, London (17 November 2021)
- Hargreaves E, 'The nature of beneficiaries' rights under trusts' (2011) 25 *TLI* 163
- Harris JW, *Property and Justice* (OUP, 2002)
- Hegel GWF, *The Philosophy of Right* (OUP, 1967)

- Hickey R, *Property and the Law of Finders* (Hart Publishing, 2010)
- Hart HLA, *The Concept of Law*, (2nd ed, OUP 1994)
- Ibbetson D, 'Sale of goods in the fourteenth century' (1991) 107 LQR 480
- International Swaps and Derivatives Association, 'ISDA Legal Guidelines for Smart Derivatives Contracts: Foreign Exchange Derivatives' (2020)
- Investing.com, 'MicroStrategy Buys 5,262 More Bitcoins with Share Sale Proceeds', *Yahoo Finance* at <https://finance.yahoo.com/news/microstrategy-buys-5-262-more-142559226.html> (accessed 1<sup>st</sup> January 2025)
- Jones MA, Dugdale AM, Simpson M, *Clerk and Lindsell on Torts* (24<sup>th</sup> edition, Sweet & Maxwell 2023)
- Law Commission of England and Wales, *Digital assets – Call for evidence* (2021)
- *Digital assets Responses to the call for evidence* (2021)
- *Digital Assets: Consultation paper* (Law Com No 256, 2022)
- *Digital assets Responses to consultation* (2022)
- *Electronic trade documents: Report and Bill* (HC 1188, Law Com No 405, 16 March — 2022)
- *Digital Assets: Final report* (HC 1486, Law Com No 412, 2023)
- *Decentralised Autonomous Organisations (DAOs) – A scoping paper* (2024)
- *Digital assets as personal property: Supplemental report and draft Bill* (HC 188, Law Com No 416, 2024)
- Lessig L, *Code: And Other Laws of Cyberspace, Version 2.0* (Basic Books, 2006).
- Litton H, *Is the Hong Kong Judiciary Sleepwalking to 2047?* (Sherriff Books, 2019)
- Liu H, 'The legal nature of blockchain securities' [2021] LMCLQ 476
- 'Digital assets: the mystery of the "link"' (2022) 3 JIBFL 161
- 'Title, control and possession in the digital asset world' [2022] LMCLQ 597
- 'Interference torts in the digital asset world (2023) (at <https://ssrn.com/abstract=4433956> (accessed 21<sup>st</sup> December 2024))
- 'Transferring legal title to a digital asset' (2023) 5 JIBFL 317
- 'Transferring legal title to a digital asset: shared and limited control arrangements (Part 2)' (2024) 4 JIBFL 251
- 'Crypto as property: a response to Professor Stevens' (2025) 141 LQR (forthcoming)
- 'Interference torts in the digital asset world' (2025) 84 CLJ (forthcoming)
- 'Transfer of title to digital assets' in Jason Allen, Simon Gleeson and Peter Hunn (eds), *Oxford Handbook of Digital Assets and the Law* (OUP, 2025) (forthcoming)
- and Chong H and Gullifer L, 'Client-intermediary relations in the crypto-asset world' in Davies P and Tan CH (eds), *Intermediaries in Commercial Law* (Hart Publishing, 2022)
- and Gullifer L, 'Financial collateral arrangements in the digital asset world' (2022) 8 JIBFL 527

- Low KFK, 'Quoines in Cryptopia: When (if ever) are Cryptoasset Exchanges Trustees?' [2020] Conv 70
- 'Trusts of Cryptoassets', City University of Hong Kong School of Law Legal Studies Research Paper No. 2020-020 (at [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3749040](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3749040) (accessed 1<sup>st</sup> January 2025))
- 'Trusts of Cryptoassets' (2021) 34(4) TLI 191
- and Mik E, 'Lost in Transmission: Unilateral Mistakes in Automated Contracts' (2020) 136 LQR 563
- McAlhone C and Wortley N, *Criminal Law – The Fundamentals* (4<sup>th</sup> ed, Sweet & Maxwell, 2016)
- McMeel G, 'The redundancy of bailment' [2003] LMCLQ 169
- McFarlane B, *The Structure of Property Law* (Hart Publishing, 2008)
- 'Identifying property rights: a reply to Mr Watt' [2003] Conv 473
- 'The Numerus Clausus Principle and Covenants Relating to Land' in Susan Bright (ed), *Modern Studies in Property Law* (Volume 6, Hart Publishing, 2011)
- 'Keppell v Bailey (1834); Hill v Tupper (1863): The Numerus Clausus and the Common Law' in Nigel Gravells (ed), *Landmark Cases in Land Law* (Hart Publishing, 2013)
- and Douglas S, 'Property, Analogy and Variety' (2022) 42 OJLS 161
- and Stevens R, 'The Nature of Equitable Property' (2010) 4 J Eq 1
- McGhee J and Elliott S (eds), *Snell's Equity* (35<sup>th</sup> ed, Sweet & Maxwell 2024)
- Merrill TW, 'Property and the Right to Exclude' (1998) 77 Neb L Rev 730
- and Smith HE, 'The Property/Contract Interface' (2001) 101 Colum L Rev 773
- and Smith HE, 'The Architecture of Property' in Hanoch Dagan and Benjamin C Zipursky (eds), *Research Handbook on Private Law Theory* (Edward Elgar Publishing, 2020) 134
- Milsom SFC, *Historical Foundations of the Common Law* (2<sup>nd</sup> ed, Butterworths 1981)
- Mossoff A, 'What is property? Putting the pieces back together' (2003) 45 Ariz L Rev 371
- Morris DZ, 'CoinDesk Turns 10: 2016 - How The DAO Hack Changed Ethereum and Crypto', *CoinDesk* at <https://www.coindesk.com/consensus-magazine/2023/05/09/coindesk-turns-10-how-the-dao-hack-changed-ethereum-and-crypto> (accessed 31<sup>st</sup> December 2024)
- Nakamoto S, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (2008) (at <https://bitcoin.org/bitcoin.pdf>, accessed 31<sup>st</sup> December 2024)
- Nagel T, *Mortal Questions* (CUP, 2012)
- Newar B, 'Wormhole Token Bridge Loses \$321M in Largest Hack So Far in 2022', *Cointelegraph* at <https://cointelegraph.com/news/wormhole-token-bridge-loses-321m-in-largest-hack-so-far-in-2022> (accessed 31<sup>st</sup> December 2024)
- Nolan D, 'Assumption of Responsibility: Four Questions' (2019) 72 CLP 123

—— ‘The Essence of Private Nuisance’ in McFarlane B and Agnew S (eds), *Modern Studies in Property Law, Volume 10* (Hart Publishing, 2019)

Nolens BN and Quinlan B, ‘Project Dynamo: CBDCs, Stablecoins, and Deposit Tokens: Wholesale Adoption Explorations and Challenges’ (BIS Innovation Hub and Quinlan and Associates, 2023)

O’Donnell A, ‘Riot Platforms Buys More Than \$500 Million in Bitcoin’, *Cointelegraph* at <https://cointelegraph.com/news/riot-platforms-buys-more-than-500-million-bitcoin> (accessed 1<sup>st</sup> January 2025)

Ooi V and Soh KP, ‘Rethinking mistake in the age of algorithms: *Quoine Pte Ltd v B2C2 Ltd*’ (2020) 31 KLJ 367

Ormerod D and Perry D (eds), *Blackstone’s Criminal Practice 2022* (OUP, 2021)

Ortynski V and Kranjc J, ‘Blockchain document transfer: understanding the technology and its uses’, *CargoX* at <https://cargox.io/content-hub/blockchain-document-transfer-understanding-technology-and-its-uses> (accessed 10<sup>th</sup> September 2024)

Palmer N and McKendrick E (eds), *Interests in Goods* (2<sup>nd</sup> ed, London: LLP Profession Publishing 1998)

Penner JE, *The Idea of Property in Law* (OUP, 1997)  
—— *Property Rights: A Re-Examination* (OUP, 2020)

Perkins J and Enwenzor J, ‘The legal aspect of virtual currencies’ (2016) 10 JIBFL 569

Poston H, ‘Hash Functions in Blockchain’, *Infosec* at <https://www.infosecinstitute.com/resources/blockchain-security-overview/hash-functions-in-blockchain/> (accessed 31<sup>st</sup> December 2024)

Prosser WL, ‘Nature of Conversion’ (1957) 42 Cornell L Rev 168

Quinlan B, Chung J and Trehan E, ‘Cracking the Code: The Evolution of Digital Assets to the Mainstream’ (Quinlan and Associates, 2021)

Quinlan B and Wills D, ‘A New Chain of Thought: Exploring the Building Blocks of the Next Digital Era’ (Quinlan and Associates, 2024)

Ramsden J, ‘Identifying and tracing the origins and flows of cryptocurrency’ (2019) 3 JIBFL 173

Redman J, ‘Before Bitcoin: 4 Early Digital Currencies and Why They Collapsed – Learning – Insights Bitcoin News’, *Bitcoin News* at <https://news.bitcoin.com/before-bitcoin-4-early-digital-currencies-and-why-they-collapsed/> (accessed 29<sup>th</sup> December 2024).

Reiff N, ‘Decentralized Autonomous Organization (DAO): Definition, Purpose, and Example’, *Investopedia* at <https://www.investopedia.com/tech/what-dao/#:~:text=A%20decentralized%20autonomous%20organization%20is,holders%20who%20collectively%20cast%20votes> (accessed 1<sup>st</sup> January 2025).

- Rostill L, ‘Terminology and Title to Chattels: A Case against ‘Possessory Title’ (2018) 134 LQR 407  
 ——— *Possession, Relative Title, and Ownership in English Law* (OUP, 2021)  
 ——— ‘The Pluralities of Property’ (2024) 44(3) OJLS 733
- Schelling TC, *The Strategy of Conflict* (Harvard University Press, 1960)
- Shaw SLK, ‘Conversion of Intangible Property: A Modest, but Principled Extension? A. Historical Perspective’ (2009) 40 VUWLR 419
- Sheehan D, ‘Digital assets, blockchains, and relativity of title’ [2024] JBL 77
- Smith H, ‘Property as the Law of Things’ (2012) 125 Harv LR 1691
- Stevens R, ‘Crypto is not property’ (2023) 139 LQR 615  
 ——— *The Laws of Restitution* (OUP, 2023)
- Stoljar S, ‘The Delivery of Chattels’ (1958) 21 MLR 27
- Sun Z, ‘\$5 wrench attacks appear to be on the rise in the crypto community’, *Cointelegraph* available at [cointelegraph.com/news/5-wrench-attacks-appear-to-be-on-the-rise-in-the-crypto-community](https://cointelegraph.com/news/5-wrench-attacks-appear-to-be-on-the-rise-in-the-crypto-community) (accessed 30<sup>th</sup> August 2024)
- Swadling W, ‘The Proprietary Effect of a Hire of Goods’ in Palmer N and McKendrick E, *Interests in Goods* (2<sup>nd</sup> ed, London 1998)  
 ——— ‘Ignorance and Unjust Enrichment: The Problem of Title’ (2008) 28 OJLS 627  
 ——— ‘Policy Arguments for Proprietary Restitution’ (2008) 28 LS 506
- Tettenborn A, ‘Reversionary Damage to Chattels’ (1994) 53(2) CLJ 326
- Turner PG, ‘Consequential economic loss and the trust beneficiary’ (2010) 69 CLJ 445
- UK Jurisdiction Taskforce, *Legal Statement on Cryptoassets and Smart Contracts* (2019)
- UNIDROIT, *Principles on Digital Assets and Private Law*
- Virgo G, ‘Justifying Necessity as a Defence in Tort Law’ in Dyson et al (eds), *Defences in Tort* (Hart Publishing, 2015) 135
- Vlacic P and Cekrljic B, ‘The legality of an electronic bill of lading | CargoX’, *CargoX* at <https://cargox.io/content-hub/legality-electronic-bill-lading> (accessed 10<sup>th</sup> September 2024)
- Waldron J, ‘Property, Justification and Need’ (1993) Can J L & Jurisprudence 185
- Wang M, Ichijo H and Xiao B, ‘Cryptocurrency Address Clustering and Labeling’ (2020) (at <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwiPzt6AueD2AhU5yYsBHUqoD8IQFnoECAgQAQ&url=https%3A%2F%2Frxiv.org%2Fpdf%2F2003.13399&usg=AOvVaw3-Ms06DTwyqzU27QP4wu2B>, accessed 23<sup>rd</sup> March 2022).

Warmke C, 'What is Bitcoin' (2021) Inquiry 1

Watt G, 'The proprietary effect of a chattel lease' (2003) Conv 61

Watts P and Low KFK, 'The Case for Cryptoassets as Property' in Sinead Agnew and Marcus Smith (eds), *Law at the Cutting Edge* (Hart Publishing, 2024) 281

Weinrib E, *The Idea of Private Law* (OUP, 2012)

'What Is Blockchain Security? | IBM', IBM at <https://www.ibm.com/topics/blockchain-security> (accessed 1st January 2025)

Winston & Strawn, 'What Is Distributed Ledger Technology (DLT)? | Law Glossary | Winston & Strawn', *Winston & Strawn* at <https://www.winston.com/en/legal-glossary/distributed-ledger-technology> (accessed 1st January 2025)

Wonnacott M, *Possession of Land* (CUP, 2006)

Wright LA, "Kidnappings and home invasions highlight need for enhanced physical security in crypto", *CryptoSlate* available at <https://cryptoslate.com/kidnappings-and-home-invasions-highlight-need-for-enhanced-physical-security-in-crypto/> (accessed 30<sup>th</sup> August 2024)

Yue F, 'Why VanEck's solana ETF application is a win for crypto – even if it's not approved | Morningstar', *Morningstar* at <https://www.morningstar.com/news/marketwatch/20240627378/why-vanecks-solana-etf-application-is-a-win-for-crypto-even-if-its-not-approved> (accessed 10<sup>th</sup> September 2024)

yyctrader, 'Axie Infinity's Ronin Bridge Exploited For More Than \$600M – "The Defiant"', *The Defiant* at <https://thedefiant.io/news/nfts-and-web3/axie-infinity-hack-600m> (accessed 31<sup>st</sup> December 2024)