

Code: And Other Laws of Blockchain[†]

Mimi Zou*

Abstract—There has been burgeoning interest among legal scholars in recent years regarding the implications of blockchain technology for the law. Two thoughtful monographs that go beyond the hyped claims of enthusiasts and cynics are Primavera De Filippi and Aaron Wright’s *Blockchain and the Law: The Rule of Code* and Kevin Werbach’s *Blockchain and the New Architecture of Trust*. While the two books have different focal points, both contain a common Lessig-inspired theme of ‘code as law’ in which decentralised blockchain networks are viewed as a regulatory ‘modality’ or ‘architecture’ with its own system of rules. However, as this article argues, blockchain is not outside the law or existing legal system. Code necessarily interacts with other modes of regulation, namely the market, social norms, and law in constraining the operation of blockchain applications such as smart contracts. This argument also situates smart contracts in a relational analysis of real-world contracting practices.

Keywords: smart contracts, blockchain and the law, relational contract theory

1. Introduction

Blockchain has attracted substantial hype in recent years. In one sense, it could join the queue of technological innovations in human history that have altered existing economic, political, and social structures. In another sense, its much-lauded potential in creating a decentralised, disintermediated, and distributed world may reside only within techno-libertarian or crypto-anarchist communities. In the early 1990s when the Internet went ‘mainstream’ with the World Wide Web, the idea of a universal and neutral network on which individuals could freely participate, implement their own systems of rules, and not be subject to the control of government and big corporations was not merely the obsession of cyber-libertarians. Questions of whether activities in cyberspace can be regulated and if so, what forms such regulation should take, sparked impassioned and dynamic debates among legal and regulatory theorists.

Among the most prominent cyberlaw scholars is Laurence Lessig, who presented (twenty years ago) an influential socio-economic theory on four modalities of regulation: the law, social norms, the market, and architecture.¹ He referred to these forces as ‘constraints’ on our actions. As Lessig posits, the regulation of something is the ‘sum of these four constraints. Changes in any one will affect the regulation of the whole. Some constraints will support others; some may undermine others... A complete view, therefore, must consider these four modalities together’.² He applies this model to describe the regulation of behaviour in cyberspace (the Internet), where the architecture is computer code.³

[†] A review of Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (HUP 2018) and Kevin Werbach, *Blockchain and the New Architecture of Trust* (MIT Press 2019).

* St Hugh’s College, University of Oxford. Email: mimi.zou@law.ox.ac.uk. With thanks to Liz Fisher and the anonymous reviewer for their very helpful advice and feedback. All errors and omissions are my own. I would also like to acknowledge the support of Oxford Law Faculty’s Research Support Fund.

¹ Lawrence Lessig, ‘The New Chicago School’ (1998) 27 *The Journal of Legal Studies* 661. This framework is also known as the ‘New Chicago School framework’ or the ‘pathetic dot theory’.

² Lawrence Lessig, *Code: And Other Laws of Cyberspace 2.0* (2006) <<http://codev2.cc/>> accessed 18 February 2020, 123.

³ Lessig (n 2) 124-125.

Lessig's theory is featured visibly in two recent monographs on blockchain by legal scholars. The first is Primavera De Filippi and Aaron Wright's *Blockchain and the Law: The Rule of Code*.⁴ The second is Kevin Werbach's *Blockchain and the New Architecture of Trust*.⁵ Both books represent notable contributions to an expanding body of scholarship on how blockchains may challenge, subvert, complement, supplement, or co-exist with the law. The authors rightly focus on public and permission-less blockchains—where the current debate on blockchain is centred—instead of permissioned distributed ledgers.⁶ The *Blockchain and the Law* pivots on the concept of 'lex cryptographia', a body of rules created by, coded in, and enforced by quasi-autonomous technological systems enabled by blockchain, which exists independently from state-created legal rules. The *New Architecture of Trust* takes the notion of trust as its core narrative. Blockchain is not 'trustless' as commonly assumed. Instead, it is the emergence of trust in a new form and its systems operate as mechanisms of coordinating and enforcing rules governing behaviour.

Both books engage in extensive discussions of smart contracts, which have been hailed as one of the most exciting applications of blockchain technology to date. Smart contracts running on a blockchain network like Ethereum can enable the creation and enforcement of an agreement autonomously through computer code. As soon as the parameters or conditions laid down in the code are met, the smart contract automatically executes the transaction in a distributed manner by the nodes in the network. Smart contracts are said to benefit from blockchain's security and tamper-resistance, which render transactions almost unalterable and irreversible. Importantly, there is no need to rely on a single centralised authority, trusted intermediary or external enforcement mechanism.

This article provides a critique of both books as well as develop their arguments relating to Lessig's regulatory modalities to analyse smart contracts. I do not intend to provide an in-depth inquiry of smart contracts with reference to existing legal frameworks, principles, and rules in particular jurisdictions.⁷ Instead, my analysis is aimed at reconfiguring our understanding of smart contracts that considers seriously real-world contracting practices and their social settings. In Sections 2 and 3, the structure and main arguments of the two books are introduced and evaluated. Weaving the books' analysis of smart contracts with insights from relational contract theorists, Section 4 presents a framework for exploring how code, alongside law, the market, and social norms may 'regulate' smart contracts.

At the onset, it should be noted that legal scholars researching this emergent and fast-evolving technology face a risky intellectual venture. To write a serious monograph on this topic runs the risks of the content being deemed 'out-of-date' upon publication or 'speculative' in describing future technological developments and regulatory consequences that may or may

⁴ Primavera De Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (HUP 2018) [hereinafter *Blockchain and the Law*].

⁵ Kevin Werbach, *Blockchain and the New Architecture of Trust* (MIT Press 2019) [hereinafter *The New Architecture of Trust*].

⁶ Permissioned ledgers are usually accessible only to approved members of a consortium and increasingly used in many commercial and government domains. Some advocates of public blockchains have argued that private ledgers should not be called 'blockchains'. This is because they are essentially centralised databases that use distributed ledger technology, the access of which is controlled by the consortium.

⁷ Other legal scholars have undertaken this endeavour. See e.g. Sarah Green, 'Smart Contracts, Interpretation and Rectification' (2018) LMCLQ 24; Jonathan G Rohr, 'Smart Contracts and Traditional Contract Law, or: The Law of the Vending Machine' (2019) 67 Cleveland State Law Review 71; a special volume on smart contracts and private law in (2018) 6 European Review of Private Law; Christina Poncibò, Larry A DiMatteo and Michel Cannarsa (eds), *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (CUP 2020). The legal profession has also sought to clarify the legal status or position of smart contracts. See, for example, the UK Jurisdiction Taskforce, 'Legal statement on the status of cryptoassets and smart contracts', 18 November 2019 <<https://technation.io/about-us/lawtech-panel/>> accessed 18 February 2020.

not eventuate. Indeed, both books are susceptible to such risks. Nonetheless, many readers will appreciate the challenging enterprise that these scholars have undertaken in analysing an emerging technology that is rapidly evolving. At the time of writing, there is already talk of ‘fourth generation blockchain’.⁸ Overall, both books do a fine job in providing a clear and accessible technical explanation as well as a lucid, interdisciplinary account of the key issues in current policy and scholarly debates on blockchain and the law.

2. *Lex cryptographia: The Rule of Code*

A. Overview

De Filippi and Wright offer a thought-provoking prediction of a ‘structural shift of power from legal rules and regulations administered by government authorities to code-based rules and protocols governed by decentralised blockchain-based networks’⁹ as blockchain technology further develops. The concept of *lex cryptographia* is used to describe such a system of algorithmic control that entails ‘order without law’¹⁰ in its architectural design. This ‘rule of code’ does not depend on geographical or jurisdictional boundaries. Importantly, it may or may not operate in accordance with the ‘rule of law’.¹¹ *Blockchain and the Law* explores the contours of this concept and concludes that blockchain cannot be effectively harnessed without new regulatory approaches.

The authors develop their thesis in five parts. Part I lays out the historical context and technical features of blockchain (Chapter 1) and how its core characteristics facilitate *lex cryptographica* (Chapter 2). Parts II-IV discuss the potential operation and effect of *lex cryptographica* arising from different use-cases. Part II discusses digital currencies and decentralised payment systems (Chapter 3), smart contracts (Chapter 4), and smart securities and derivatives (Chapter 5). Part III examines emerging use-cases in information systems, including repositories for public records (Chapter 6) and information storage, transfer and online communications (Chapter 7). In Part IV, the authors explore the possibility of decentralised organisational structures in coordinating social and commercial activities (Chapter 8). Decentralised autonomous organizations (DAOs) represent the most advanced type of such structures (Chapter 9), which can even enable connected devices in Internet of Things (IoT) systems to autonomously transact value with one another (Chapter 10). Part V proposes how blockchain applications can be regulated (Chapters 11) and how *lex cryptographica* can be used for regulation (Chapter 12).

The book provides valuable insights into the tensions between different and often competing modes of regulation, actors and institutions. However, the structure of key arguments tends to be framed in a binary, oppositional manner. Code is pitted against the law. Regulation is pitted against innovation. Decentralised organisations based on blockchain are pitted against centralised institutions of the state, banks, and big corporations. This dichotomisation is further reflected in the dual-nature narrative (‘blockchain for good’ versus ‘blockchain for bad’) underpinning the book’s analysis of various use-cases.

There are analogous regulatory issues arising from current debates on other technologies. *Lex cryptographica* poses similar questions regarding the relationship of the law to decentralised networks and ‘self-governing’ online communities when the Internet first became

⁸ Vinay Nair, ‘What Will the Fourth Generation of Blockchain Look Like?’ (Hackernoon, 8 April 2019) <<https://hackernoon.com/what-will-the-fourth-generation-of-blockchain-look-like-daa5a4e90c59>> accessed 16 February 2020.

⁹ De Filippi & Wright (n 4) 7.

¹⁰ *ibid* 5.

¹¹ *ibid* 7.

a mass medium. While De Filippi and Wright acknowledge some parallels,¹² there could have been greater engagement with earlier scholarly debates on regulating the Internet. This would highlight the important point that the challenges are not unique to blockchain.¹³ Likewise, salient insights from debates on regulating other major techno-social developments of our time (such as the ascendancy of machine learning and the platform economy) could have been included. Understandably, addressing all these issues in detail would be outside the scope of the book. Nevertheless, the reader would have appreciated a deeper discussion of some of the key interconnecting issues (such as trust, privacy, algorithmic discrimination, and democratic governance) from past and ongoing debates on other novel technologies.

B. *The ‘dual nature’*

Understanding the technological components of blockchain is crucial to understanding these systems that are based on *lex cryptographica*. De Filippi and Wright identify blockchain’s core characteristics.¹⁴ First, blockchain is disintermediated and transnational. It does not require a centralised party to operate across the globe. Second, it is resilient and resistant to alteration (‘tamper-resistant’) due its distributed nature and the use of consensus mechanisms. Third, blockchain’s use of cryptographic techniques enables the storage of non-repudiable data while maintaining the transparency of the metadata of all transactions. Fourth, blockchain allows for pseudonymity. Participants can engage in transactions without revealing their identity. Fifth, incentivization and payoff structures reward those who maintain the network. Sixth, consensus mechanisms enable the distributed network to coordinate its activities without a centralised authority or an intermediary. Finally, there is ‘autonomy’ in that blockchains facilitate the execution of computer code that is entirely independent of any single party.

De Filippi and Wright point out that blockchain protocols piggyback on existing Internet technologies in the TCP/IP model, which conceptualises the Internet into five layers: physical, data link, network, transport, and application.¹⁵ Blockchain sits between the transportation and application layers and importantly, enables protocols and services that are capable of ‘implementing their own system of rules—*lex cryptographica*—enforced by the underlying protocol and smart contracts’.¹⁶ Unlike the centralised control over algorithms presently exercised by online intermediaries, new self-contained and autonomous systems relying on *lex cryptographica* can be designed to make it immensely hard for any single entity to control. However, these code-based rules may also constrain human behaviour and choice to our detriment.¹⁷

The combination of the above characteristics results in the ‘dual nature’ of blockchains: their potential to be used for good and for bad.¹⁸ This theme is carried throughout the book as the authors discuss different uses of the technology. As mentioned earlier, this binary narrative can leave the reader with the impression of a slightly reductionist framing of the regulatory challenge, namely, how to maximise blockchain’s societally advantageous uses while avoiding its facilitation of unlawful activities. The systematic listing of ‘good versus bad’ in each chapter detracts from a more nuanced discussion of how blockchain’s various characteristics challenge the substance, structure, and enforcement of the law and legal system.

Several use-cases are examined in detail to illustrate blockchain’s dual nature. For example, blockchain-based cryptocurrencies and payment systems are claimed to benefit countries with

¹² *ibid* 174-175.

¹³ *ibid* 206-207.

¹⁴ *ibid* 33-45

¹⁵ *ibid* 47-49.

¹⁶ *ibid* 50.

¹⁷ *ibid* 55-56.

¹⁸ *ibid* 46.

weak or underdeveloped payment and remittance infrastructures, due to the disintermediated and transnational nature of blockchain and its ability to transfer value. However, these systems may undermine anti-money laundering laws (because of blockchain's distributed, pseudonymous characteristics) and privacy laws (given the transparency of transactional data). The widespread adoption of cryptocurrencies also risks destabilising the financial system.¹⁹

Blockchain-based smart contracts can be used to create digitalised financial agreements that are settled and cleared almost instantaneously without a need for third-party administration. Where third parties are required (for example, in derivatives trading), external sources known as 'oracles' can help adjust contractual performance. Smart securities and derivatives can reduce counterparty risk and disputes as well as boost efficiency and transparency of financial markets. However, they lack the benefits of financial intermediaries such as providing insurance to market participants and acting as buffers in times of crisis. In envisioning 'decentralised capital markets', De Filippi and Wright assert that financial products and marketplaces relying on *lex cryptographica* would be agnostic to existing financial regulations.²⁰

Blockchain's tamper-resistance further raises the possibility of use for registries and repositories for public records that require verification of the data's authenticity and integrity, such as property transfers, marriage records, corporate filing, as well as the management of sensitive data such as health data. However, blockchains are not immune from corruption and malicious attacks. Furthermore, the public storage of data in transparent blockchain can entail privacy risks for individuals. Data privacy issues are recurrent in De Filippi and Wright's assessment of blockchain's shortcomings. Yet, there is little reference to the differences in data protection and privacy regulations around the world, which would seem pertinent to a proper evaluation of the varying types and degrees of risks different jurisdictions may face.²¹

At times, the reader is left with the impression that many use-case illustrations are based on hypotheticals. For example, the authors claim that 'Bitcoin could prove to be a complement to, or even a substitute for, traditional payment systems in countries lacking stable currencies'.²² Equally speculative is the book's analysis of censor-resistant communication systems on blockchain, which the authors claim would generate free flow of information but risk copyright infringement and distribution of harmful speech and national security information. From the reader's perspective, hypotheticals (however well-crafted and interesting) are just not as compelling as real-world examples. One needs to be wary of the constant stream of imaginative ideas about prospective blockchain applications, but not many get even close to development, let alone implementation. The authors fleetingly acknowledge this point in their conclusion when they warn against the premature regulation of 'new and unexpected applications that have not yet been fully explored or discovered'.²³

C. *Decentralised organisations*

The strongest manifestation of *lex cryptographica* is in new forms of decentralised organisations that rely on blockchain and smart contracts 'as their primary or exclusive source of governance'.²⁴ These organisations can coordinate members' activities towards a shared social or economic goal 'in a transparent and inclusive manner, and the code could be designed by and for the benefit of its participants rather than a central intermediary'.²⁵ De Filippi and

¹⁹ *ibid* 61-71.

²⁰ *ibid* 96-98.

²¹ For an excellent analysis of blockchain regulation in EU law, see Michelle Finck, *Blockchain Regulation and Governance in Europe* (CUP 2019).

²² De Filippi & Wright (n 4) 63.

²³ *ibid* 209.

²⁴ *ibid* 136.

²⁵ *ibid* 139.

Wright point out the more obvious challenges of decentralised organisations, such as security vulnerabilities, lack of limited liability for participants, and the broader hurdles of subjecting these organisations to legal regulation. However, the authors could engage more with current debates on whether experimentations in decentralised blockchain governance may pave the way for techno plutocracies.²⁶ The concentration of power within blockchain systems is an important debate, especially if *lex cryptographica* will ultimately be designed by Silicon Valley.

Then there are Decentralized Autonomous Organizations (DAOs), governed entirely by artificial intelligence or other forms of autonomous code. A futuristic vision of DAOs entails smart contracts that enable Internet-connected devices to autonomously interact or transact value with each other without any human intermediaries. De Filippi and Wright make a case for designing pre-deterministic rules governing DAOs to ensure ‘certainty for individuals and machines to coordinate themselves—even if they do not know or trust one another’²⁷ and to reduce opportunity for opportunistic behaviour. Once again, the authors postulate the regulatory difficulties posed by DAOs based on *lex cryptographica*, including jurisdictional issues and a lack of legal personhood. However, more could be said about the pitfalls of automated and algorithmic governance in evaluating the desirability of DAOs. The reader’s appetite for a more critical examination of the risks relating to ‘emancipated, AI-driven machines’²⁸ running on blockchains remains unsatisfied.

De Filippi and Wright draw heavily on a US-influenced economic analysis of law to evaluate blockchain-enabled decentralised organisations. For example, Coase’s transaction cost theory is the backdrop for their account of how these structures can help firms operate more efficiently, reduce operational costs, and improve internal control while enhancing transparency. While this ‘Law and Economics’ approach is popular in some quarters, it may not necessarily find a highly receptive audience outside North America.²⁹ And yet, there is surprisingly little reference to crypto-economics in the book (which, in comparison, Werbach examines in more detail in his book).³⁰ Some key aspects of blockchain’s infrastructure have been developed based on game theory models, which incorporate a range of economic incentives in its design. For example, under the consensus mechanisms that make blockchain’s security and tamper-resistance possible, it is more costly for participants to act dishonestly than it does to act honestly.³¹

D. Regulation of and by blockchain

One of the main ideas in *The Blockchain and Law* concerns ‘code as law’. The authors consider how public and private actors can use blockchain to create their own system of rules and regulations based on self-executing code: ‘With blockchains, payment systems, financial markets, information systems, and—more generally—the allocation of labor between people

²⁶ See, e.g. Wessel Reijers, Iris Wuisman, Morshed Mannan, Primavera de Filippi, Christopher Wray, Vienna Rae-Looi, Angela Cubillos Vález and Liav Orgad, ‘Now the Code runs itself: On-chain and Off-chain governance of blockchain technology’ (2018) 37 *Topoi* 1.

²⁷ De Filippi & Wright (n 4) 151

²⁸ *ibid* 169.

²⁹ Nuno Garoupa, ‘Updating the Law and Economics of Legal Parochialism’, in Alain Marciano, Giovanni Battista Ramello (eds) *Law and Economics in Europe and the U.S.: The Legacy of Juergen Backhaus* (Springer 2016) 171-184.

³⁰ De Filippi has written another paper with other co-authors on crypto-economics. See: Sinclair Davidson, Primavera de Filippi and Jason Potts, ‘Economics of Blockchain’ (Public Choice Conference, Fort Lauderdale, May 2016) <10.2139/ssrn.2744751> accessed 1 February 2020.

³¹ Joseph Abadi and Markus K. Brunnermeier, ‘Blockchain Economics’, NBER Working Paper No. 25407, 31 August 2019 <https://scholar.princeton.edu/sites/default/files/markus/files/blockchain_paper_v7a.pdf> accessed 30 January 2020.

and machines can be governed by technical rules'.³² However, as the authors could have made clearer throughout the book, notwithstanding the operation of *lex cryptographica* in blockchain systems, blockchains are *not* beyond the law or the legal system. Regrettably, the most interesting aspects of the book concerning regulation (which also have the greatest relevance for policymakers) are squeezed in two relatively slim chapters at the end.

De Filippi and Wright draw on Lessig's theory on regulatory modalities to argue that the state can regulate blockchain through the law, social norms, market intervention, and code. The state can impose legal rules on end users, developers, cryptocurrency exchanges, miners, hardware manufacturers, and other actors in blockchain networks. The state can also intervene through the market such as buying and selling cryptocurrencies or seek to influence social norms established within a blockchain-based community. Examples of the state regulating through code ('architecture') include requiring certain functions to be inserted into the code or having code certification procedures. The authors note the trade-offs associated with various approaches of state regulation, with a focus on the potential for regulation to stifle innovation and technological development. However, the authors could have embraced a more critical account of regulation which recognises the significance of the design and choice of regulatory instruments in stimulating and aiding technological innovation in different settings.³³

The authors also envisage the incorporation of legal rules into computer code for regulating behaviour, albeit with practical and normative challenges. The decentralised, transparent, and tamper-resistant characteristics of blockchain, combined with self-executing smart contract code, can allow governments and private actors to create and implement their own systems of rules and regulations.³⁴ De Filippi and Wright discuss the efficiency benefits of utilising blockchain as 'regulatory technology' whereby governments could transpose some laws into autonomous code-based rules. The automatic enforcement of these rules can bring benefits in terms of efficiency, consistency, and predictability.

As code in decentralized blockchain-based systems and applications assume the role and functionality of legal rules, the book raises the possibility of the 'rule of code' supplanting the rule of law that governs the current regulatory framework. Nevertheless, the authors maintain that 'blockchain technology does not spell the end of the rule of law as we know it'.³⁵ This is because governments can still use the four modalities to regulate new technology, especially since there will be individuals and entities in blockchain systems that are subject to the rule of law. Here, the authors' understanding of the 'rule of law' is focused on legal rules 'based on geographical boundaries',³⁶ which seems somewhat narrow. While the book has little room for jurisprudential explication, this concept could be better teased out given its centrality to the authors' thesis.

3. The New Architecture of Trust

A. Overview

Werbach's book deploys the concept of the 'architecture of trust' to analyse the relationship between blockchain and law, regulation, and governance. As the author puts it, 'when trust in centralised power structures is waning, the blockchain's trustless trust offers a compelling alternative'.³⁷ The 'crisis of trust' is discussed throughout the book, contextualising the origins

³² De Filippi & Wright (n 4) 55.

³³ Jonathan Wiener, 'The regulation of technology, and the technology of regulation' (2004) 26 *Technology in Society* 483.

³⁴ De Filippi and Wright (n 4) 196-199.

³⁵ *ibid* 208

³⁶ *ibid* 206.

³⁷ Werbach (n 5) 246.

of blockchain and its potential direction of travel. A vast majority of our economic transactions have traditionally relied on entrusting centralised institutions such as governments, large banks and corporations. Public trust in these institutions quickly eroded during the global financial crisis of 2007-2008. This was when Bitcoin was founded as ‘a system for electronic transactions without relying on trust’.³⁸ Such a system would allow participants to transact value and trust the data recorded on a decentralised, distributed ledger without trusting any person or entity for validation.

One of the books’ central arguments is that the blockchain ‘does not eliminate the need for trust. It represents, rather, the emergence of trust in a new form’.³⁹ Werbach provides numerous examples where blockchain’s promise of ‘trustless trust’ has broken down. Others have also pointed out that substantial trust in a range of intermediaries involved in the blockchain ecosystem is still required.⁴⁰ Another main argument of the book is that blockchain cannot function without the law. Law will be a key factor in determining whether blockchain systems and applications scale over time. For Werbach, the most important contribution of the law to blockchain’s development is not a set of rules but the ‘jurisprudential discipline of rule-making and rule enforcement’ or ‘governance’.⁴¹ Law and code can work together to promote trust.

Part I (Chapters 1-4) lays out the origins, features, and functions of blockchain, as well as the nature of its ‘trust architecture’. The reader is introduced to the contemporary ‘trust crisis’ and how ‘blockchain trust’ differs from other trust relationships (Chapter 1). Blockchain is seen by its advocates to solve this crisis, through Bitcoin (Chapter 2) and other applications such as smart contracts (Chapter 3). Blockchain offers several value propositions (Chapter 4). In Part II (Chapters 5-9), Werbach argues that the solutions to blockchain’s trust challenge lie in governance, law, and regulation. Blockchain’s most lauded ‘trustless’ features also provide reason to distrust them (Chapter 5). While blockchain networks and applications offer substantial benefits, there are also many dangers (chapter 6). Governance is critical for blockchain’s success, which involves government-defined legal regimes and private means of regulating behaviour (Chapter 7). When blockchain interacts with law, the former can supplement, complement, or substitute the latter (Chapter 8). Werbach argues that governments can, will, and should have oversight over blockchain networks (Chapter 9). Part III explores how to bridge the gaps between law and blockchain, with proposals of governance mechanisms and hybrids of code and law (Chapter 10). If blockchain succeeds in creating the ‘new architecture of trust’, it may revigorate a more decentralised version of the Internet (Chapter 11).

Compared to De Filippi and Wright, Werbach offers a more modest prognosis of blockchain’s potential impact. Like other technologies in history that were deemed as ‘revolutionary’ at the time of their advent, their longer-term developments did not turn out as expected. He asserts that blockchains have considerable value propositions, namely decentralised control, creation of a single trusted record, collaboration across organisational boundaries, and tokens of value. However, Werbach also highlights the limitations of these propositions. He questions, for example, the value of crypto tokens based on their actual utility and the frenzy around ICOs.⁴² Given the technology’s novelty and immaturity, we should be

³⁸ Satoshi Nakamoto, ‘Bitcoin: A Peer-to-Peer Electronic Cash System’ (31 October 2008) 8 <<https://bitcoin.org/bitcoin.pdf>> accessed 1 December 2019.

³⁹ Werbach (n 5) 3.

⁴⁰ See e.g. Angela Walch, ‘In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains’ in Philipp Hacker, Ioannis Lianos, Georgios Dimitropoulos, and Stefan Eich (eds) *Regulating Blockchain: Technological and Legal Challenges* (OUP 2019) ch 3. Walch suggests that developers who propose or advocate for changes to the code base of public blockchains exercise power over users in a way that appears like the power that a fiduciary has over a beneficiary.

⁴¹ Werbach (n 5) 11.

⁴² *ibid* 75-91.

assessing its distinctive advantages in the longer run. Werbach considers this ‘quantum thinking’ essential in current debates on blockchain to avoid exaggerated, premature views in the short term.

On occasion, Werbach fails to elaborate on issues that he notes in passing as ‘important’. For example, he mentions Frank Pasquale’s concept of a ‘black box society’⁴³ when commenting on the significant dangers of algorithmic systems, but he does not further articulate Pasquale’s meaning of this idea. Werbach cites many different works such as those of Carola Perez (speculative bubbles), Ronald Coase (theory of the firm), Frank Knight (uncertainty and risk), and Elinor Ostrom (community economy and collaboration) among others throughout the book. However, salient insights from these references are often presented without much analysis or explanation of underlying theories (though lengthier discussions would understandably fall outside the scope of this book).

B. *Types of trust architecture*

Werbach attempts to define ‘trust’ as ‘confident vulnerability’, which entails having a positive expectation about the other party (e.g. to undertake an action important to the trustor) and a ‘willingness to be vulnerable’ in which the trustor gives up power to others.⁴⁴ He identifies four types of trust architectures.⁴⁵ First, there is peer-to-peer trust that usually emerges from moral and reputational drivers of trust in human relationships. The second is Leviathan trust, which entails institutional trust that enables parties to enter into an agreement based on trusting the state or another centralised authority to enforce the agreement and resolve any disputes. Third, intermediary trust arises where parties do not need to trust each other but a trusted intermediary. The fourth type is distributed trust. Blockchain represents this ‘new architecture of trust’, whereby it ‘severs the connection between institutional actors and the trustworthy system’.⁴⁶ In other words, users can trust the output of a system without needing to trust any of individual actors within the system.

‘Blockchain trust’ has several important features. First, distributed trust is designed within blockchain where it is not necessary to trust any single party. Second, crypto-economic incentives are structured to ‘make honesty the winning strategy’⁴⁷ among parties in public blockchain networks. Third, as more blocks are being added, it becomes more difficult to alter the chain. When it comes to transparency, blockchains use open source software and transactions are public and traceable. Cryptography is used to preserve anonymity. Werbach explains how Bitcoin’s technical features solve some key challenges of trust in computer networks, such as the ‘Byzantine Generals Problem’ (in which a system’s actors must agree on a concerted strategy but some information they receive may be unreliable or faulty) and ‘sybil attacks’ (where a node can control a peer network by creating multiple fake identities).

C. *In Code We Trust?*

Ken Thompson, the co-creator of the Unix operating system, once famously remarked: ‘You can’t trust code that you did not totally create yourself. (Especially code from companies that employ people like me.)’⁴⁸ Even when it is open source, could you trust the code that you do not have the knowledge to review and audit? And even if you do have the expertise, Thomson

⁴³ Ibid 109.

⁴⁴ Ibid 25.

⁴⁵ Ibid 25-31

⁴⁶ Ibid 30.

⁴⁷ Ibid 100.

⁴⁸ Ken Thomson, ‘Reflections on Trusting Trust’, 1983 Turing Award Lecture (1984) 27 Communications of the ACM 761, 763.

argues that ‘No amount of source-level verification or scrutiny will protect you from using untrusted code’.⁴⁹ I have argued elsewhere that users place immense trust in the hands of the coders and the developers of the software underlying smart contracts.⁵⁰ Trusting coders including trusting their ability and intention. Given the potential power imbalance between users and developer communities (and software companies), this may over time lead to distrust amongst users in the system. A lack of recourse in the event of bugs or malfunctions cropping up in the code, especially if they go undetected, can exacerbate such distrust.⁵¹

There are also various risks associated with algorithmic trust underlying blockchain-based systems. To date, the increasing use of algorithmic decision-making and rule enforcement in a wide range of settings by public and private actors cannot be said to have realised grand aspirations of neutral and incorruptible judgment and enforcement of rules. Werbach briefly notes the problems of privacy, manipulation, and reinforcement of societal biases.⁵² Other scholars have pointed out numerous regulatory challenges arising from a lack of transparency in algorithmic systems and the difficulties in addressing encoded biases.⁵³ Werbach is right to draw attention to the additional dangers of machine learning in these systems,⁵⁴ the opacity of which makes it extremely hard for humans to properly construe and review the algorithms. Another point that could have strengthened this argument is the limited ability for users to challenge and seek effective redress for the impact of these decisions, which further undermines algorithmic trust.

For blockchain users to trust the cryptography, protocols, software, and network, such trust must be rooted in broader governance systems. Werbach presents a convincing argument that trust is best promoted through external oversight such as appropriate legal regulation and compliance mechanisms as well as internal systems of governance within blockchains. Applications and services built on blockchain will not scale without adequate governance. For example, smart contracts need feasible dispute resolution mechanisms which combine recourse to traditional legal mechanisms as well as new decentralised approaches.

As such, institutional sources of trust cannot be replaced by trust in code. For Werbach, the law can cultivate trust ‘because it is an institution, not just a set of formal rules’.⁵⁵ The legal system is, on the whole, a flexible and adaptable institution. The procedures underlying the law’s implementation, such as court decisions, legislation, administrative actions, have formal and informal bases for legitimacy. Here, Werbach could have elaborated on the importance of legitimacy in systems of governance, especially where the rules of the system are created and enforced through democratically accountable institutions and processes. A question left unanswered in this book is the legitimacy of blockchain-enabled private modes of regulation (or De Filippi and Wright’s notion of *lex cryptographia*) vis-à-vis the legitimacy of the law.

D. Cryptogovernance

The book adopts Lessig’s argument that code is a regulatory modality on its own right.⁵⁶ Werbach modifies Lessig’s four modalities to capture blockchain’s special attributes. First, the

⁴⁹ *ibid* 763.

⁵⁰ Mimi Zou, Grace Cheng and Marta Soria Heredia, ‘In Code We Trust? Trustlessness and smart contracts’ (2019) *Computers and Law* <https://www.scl.org/articles/10493-in-code-we-trust-trustlessness-and-smart-contracts> accessed 1 February 2020.

⁵¹ *Ibid*.

⁵² Werbach (n 5) 109-110.

⁵³ Jack M. Balkin, ‘The Three Laws of Robotics in the Age of Big Data’ (2017) 78 *Ohio State Law Journal* 1217; Lilian Edwards and Michael Veale, ‘Slave to the Algorithm: Why a Right to an Explanation Is Probably Not the Remedy You Are Looking for’ (2017) 16 *Duke Law and Technology Review* 18.

⁵⁴ Werbach (n 5) 110.

⁵⁵ *ibid* 140.

⁵⁶ *ibid* 153.

distinctive architectural element of blockchains is cryptography. Second, self-interest represents the market, which capture the crypto-economic incentives and the fact that many decisions made within blockchain networks do not involve actual market transactions. Third, Werbach puts trust in the place of Lessig's social norms, asserting that trust is 'the factor that makes (social) norms possible'.⁵⁷ Finally, there is law. Werbach further categorises the four modalities along two axes: whether they are grounded in formal/mathematical terms or human language; and whether they convey a system of rules or human motivation. The challenge for cryptogovernance is how to merge the four modalities of cryptography, self-interest, trust, and law.

Werbach proposes a framework for regulation in which three questions should be addressed by policymakers.⁵⁸ The first is whether the blockchain system or application created is for a legitimate purpose. Second, are there alternative means of achieving public policy goals (such as self-regulation)? Finally, what are the costs and benefits of regulatory action? As to the question of *how* regulators should act, he suggests two ways of connecting blockchain and the law. First, law could be made to 'operate more consistently with governance through software code',⁵⁹ such as regulatory sandboxes and safe harbours, modular contracts, and adaption of fiduciary responsibility for blockchain networks. Second, code can be made 'more law-like', which entails blockchain systems becoming 'more hospitable to legal enforcement'.⁶⁰ This could be achieved through integrating legal terms and enforcement mechanisms into smart contracts and having on-chain governance systems that are more akin to a human-based legal regime. These proposals avoid the trap of being prescriptive, which is important given that the technology as well as its practical and legal implications are still in flux.

The book concludes by drawing some powerful parallels between the Internet and blockchain in discussing these technologies' relationship to law and governance. As Werbach puts it, 'The cyber libertarians of the 1990s were wrong that the Internet could escape the clutches of territorial legal regimes, but they were right that governments and courts should take the Internet's potential seriously'.⁶¹ What is more, the book rightly draws attention to the power dynamics in the centralization of the Internet that is now dominated by a small handful of trusted intermediaries whose 'power is inherently corrupting'.⁶² If blockchains potentially scale and become adopted as trustworthy ledgers, they could function as a new layer in the Internet's structure. This would reduce opportunities for proprietary control by dominant Internet platforms and promote an open environment for decentralised applications on the Internet that would boost innovation and empower individuals. Without robust cryptogovernance mechanisms that induce trust, Werbach warns that blockchain, like the Internet, may not remain a 'technology of openness'.⁶³

4. Smart Contracts: Law, Code, and Trust

A. Smart contracts as 'law'

The concept of smart contracts preceded the arrival of blockchain technology. Perhaps the most cited definition is that of Nick Szabo in 1994 when he described smart contracts as

⁵⁷ *ibid* 154.

⁵⁸ *ibid* 194.

⁵⁹ *ibid* 204.

⁶⁰ *ibid* 212.

⁶¹ *ibid* 226.

⁶² *ibid* 237.

⁶³ *ibid* 240.

‘computerized transaction protocol that executes the terms of a contract’.⁶⁴ Szabo further explains that:

The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries. Related economic goals include lowering fraud loss, arbitration and enforcement costs, and other transaction costs.⁶⁵

As both books observe, blockchain has made Szabo’s ideas on smart contracts practically significant. This is particularly the case in respect of the Ethereum platform that could support ‘any application that can be coded in software’.⁶⁶ Blockchain-based smart contracts not only memorialise the details (all or parts) of an agreement between contracting parties in code but also automate the execution and enforcement of its terms on the distributed ledger, without an intermediary.

De Filippi and Wright examine the idea of ‘smart contracts as legal contracts’ in their book.⁶⁷ They identify some resemblances between smart contracts and traditional written agreements in legal prose, such as the need for parties to reach agreement on the terms which may be memorialised in whole or in part in code and the possibility for parties to seek redress from a court to reverse the effects of the smart contract. The agreement underlying the smart contract will still be subject to relevant laws. The primary difference is smart contracts’ autonomous enforcement of encoded obligations whereby no single party, by default, can control or halt the program’s execution. In doing so, smart contracts can reduce parties’ need for monitoring performance and the risk of opportunistic behaviour.⁶⁸ The precision, clarity, and modularity of code are said to decrease contractual ambiguity and the potential for misinterpretation.⁶⁹

As De Filippi and Wright put it, smart contracts’ purported advantages of automated and guaranteed execution may ‘lead to excessive rigidity and an inability to keep pace with changing circumstances’.⁷⁰ At the same time, the law’s shortcomings with regards to ambiguity and uncertainty are ‘also its greatest strengths’, since these attributes enhance the flexibility and adaptability of contractual rules.⁷¹ Parties can think more carefully about smart contract design and use technical mechanisms such as human oracles to reduce the rigidity of these self-enforcing agreements. However, it will not eliminate the real possibility for smart contracts to undermine parties’ desire to preserve some flexibility, particularly in ongoing contracting relationships and where obligations may change in the course of the relationship.⁷² I shall expand on these insights from relational contract theory later on to explore the role of legal contracts in day-to-day business transactions.

B. Smart contracts as a ‘new architecture of trust’

As Werbach explains: ‘[I]n any transaction, there are three elements that may be trusted: the counterparty, the intermediary, and the dispute resolution mechanism. The blockchain tries to replace all three with software code’.⁷³ The private digital keys of smart contracts can facilitate

⁶⁴ Szabo, ‘Smart Contracts’ (1994)

<<http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>> accessed 1 February 2020.

⁶⁵ *ibid.*

⁶⁶ Werbach (n 5) 55.

⁶⁷ De Filippi and Wright (n 4) ch 4.

⁶⁸ *ibid* 80-81.

⁶⁹ *ibid* 81-82.

⁷⁰ *ibid* 209-210.

⁷¹ *ibid.*

⁷² Zou, Heredia-Soratia, Cheng (n 50); De Filippi and Wright (n 4) 84.

⁷³ Werbach (n 5) 29.

the entry into contractual relationships with others with whom we have no prior social ties or experience in interacting as well as whose reputation is unknown, thereby reducing the need for interpersonal trust between contracting parties.⁷⁴ Smart contracts also remove the need for a trusted intermediary in a contractual relationship such as a bank or guarantor, since the transaction platform is a distributed network of nodes. Predefined algorithms that self-execute do not require recourse to traditional institutions such as courts to resolve contractual disputes and enforce the parties' obligations.

However, blockchain-based smart contracts raise a new set of trust issues. As Werbach argues, 'blockchain is not entirely trustless. It may promote justified confidence, but not without vulnerability'.⁷⁵ Both books analyse a well-known example of vulnerability in smart contracts: the attack on The DAO, a decentralised autonomous organisation that operated like a venture capital fund. A coded structure capable of self-governance and autonomous decision-making, The DAO was constructed by a myriad of smart contracts that 'took the place of law, intermediaries, and personal relationships as the foundation for trust'.⁷⁶ It was hacked weeks after its launch through the exploitation of several vulnerabilities in its code, resulting in the siphoning of more than a third of its funds. The DAO hack itself was entirely legitimate according to the smart contract code.

It was only through the 'centralised' leadership of core developers in the Ethereum community that the siphoned funds were retrieved through creating a hard fork adopted by a majority of mining nodes. The hard fork retroactively invalidated transactions that were formally valid within the code. The promise of blockchain's trust architecture was greatly undermined by The DAO attack, not only because of the security vulnerabilities that gave rise to the attack but also the hard fork response that exposed the limits of blockchain's distinctive characteristics such as immutability as well as the idea of decentralised trust. In comparison to public blockchains, the increasing adoption of permissioned (private) ledgers by governments and companies can be partly explained by the fact that permissioned ledgers 'maintain a residual level of trust in the identity of network participants'.⁷⁷

The debacle of The DAO attack exposed the fact that smart contracts cannot discern the intention of a bona fide party from that of a hacker and will execute according to the pre-determined rules of the smart contract code. At the same time, it demonstrated a shifting of trust from traditional intermediaries to a core group of developers within the system. The hard fork response to The DAO attack caused much controversy in the blockchain community, since there was no democratic decision-making process in place and those who created the hard fork had substantial 'skin in the game'. Trust in smart contracts require external mechanisms of governance that go beyond a leap of faith in code and coders. As Werbach eloquently states:

In the technology world, many prefer to ignore the ways that software architecture grants the authority to shape behaviour. The power of courts and regulatory agencies is easy to see; that of code and its masters, less so. Yet both are power regulators. Poorly designed code can be as harmful as poorly designed law.⁷⁸

C. *The function of contracts*

An important idea put forward by both books is that of 'code as law'. Some have claimed that the development of smart contracts may render traditional contracts less relevant.⁷⁹ This raises the question of the actual function of contract law in business transactions and market exchange.

⁷⁴ Zou, Heredia-Soriatia, Cheng (n 50).

⁷⁵ Werbach (n 5) 31.

⁷⁶ *ibid* 67.

⁷⁷ *ibid* 60.

⁷⁸ *ibid* 233.

⁷⁹ Alexander Savelyev, 'Contract law 2.0: 'Smart' contracts as the beginning of the end of classic contract law' (2017) 26 *Information & Communications Technology Law* 116.

A preeminent relational contract theorist, Stewart Macaulay, has argued that non-contractual mechanisms such as social norms and practices played a more important role in market transactions than the contractual relationship. Parties entered into contracts often for other reasons (such as planning transactions or control within organisations) besides the prospect of its enforceability before a court. Nevertheless, contracts will be used where and when it is useful or there are no other alternatives.⁸⁰

Hugh Collins builds on the rich empirical research on contractual practices spurred by Macaulay's work.⁸¹ He questions the conventional view that the law of contract is a key component for establishing bonds of trust that underpin a market economy. This common account of the construction of social order posits that courts (as agencies of the state) regulates contractual behaviour through a system of rules and sanctions, thus enabling trust between strangers in undertaking transactions in the marketplace.⁸² Collins argues that that real-world contracting consists of three components. The first is the economic deal underlying a particular transaction. Second, there is the relationship between the parties. The third is the formal contract itself, which embodies the parties' legal rights and obligations. When parties enter into a contract, their behaviour is not usually guided around a legal framework. Instead, their priority may be to sustain the business relationship and ensure that the deal is successful.⁸³ Collins noted that firms used contracts as a form of insurance in case the business relationship broke down.⁸⁴

Among legal scholars writing on smart contracts, the influence of relational contract theories can be found in Karen Levy's work. Levy has argued that the enthusiasm over smart contracts' features of self-execution and automated enforcement ignores the social norms and relational contexts surrounding contracting practice.⁸⁵ Like Macaulay and Collins, she considers contracting practices whereby parties deliberately include prima facie unenforceable or vague terms, or intentionally ignore contractual breaches. Levy's line of argument follows on from Macaulay's study of how the 'paper-deal' (what is written in the contract) often differs from the 'real-deal' in contractual relationships. Contracting parties choose to rely upon relational norms behind the contract rather than opt for strict enforcement of the contractual terms.⁸⁶

Levy considers the function of contracts as 'social resources', which are used by people to manage their relationships. As she puts it, 'Contracts are deeply social tools as well as legal ones'.⁸⁷ She presents three examples of contracting practices to illustrate this idea: where parties draft/accede to terms that they know or suspect to be unenforceable, where parties draft/accede to purposefully vague terms, and where parties decide not to enforce an enforceable agreement. The social aims underpinning these practices include setting norms for future behaviour, facilitating stable and flexible long-term relations, and providing a strategic resource for bargaining in the shadow of the law. Enthusiasm for the 'transformative' potential of smart contracts based on their 'careful prespecification of terms and automated enforcement of obligations'⁸⁸ ignores the social complexities of contracting.

D. *Forces 'constraining' smart contracts*

⁸⁰ Stewart Macaulay 'Non-contractual relations in business' (1963) 28 *American Sociological Review* 45.

⁸¹ Hugh Collins, *Regulating Contracts* (OUP 1999).

⁸² *ibid* 3-4.

⁸³ *ibid* 127-48.

⁸⁴ *ibid* 256-86.

⁸⁵ Karen EC Levy, 'Book-Smart, Not Street-Smart: Blockchain-Based Smart Contracts and the Social Workings of Law' (2017) 3 *Engaging Science, Technology, and Society* 1

⁸⁶ Stewart Macaulay 'The Real Deal and the Paper Deal: Empirical Pictures of Relationships, Complexity and the Urge for Transparent Simple Rules' (2003) 66 *MLR* 44.

⁸⁷ Levy (n 85) 10.

⁸⁸ *ibid*.

These above insights are salient to the concern of De Filippi and Wright and Werbach with how smart contracts intersect with other regulatory modalities, particularly the law. Here, I suggest a reconfiguration of our understanding of smart contracts to include four intersecting forces that have varying degree of importance in each transaction: the parties' relationship (social norms), the economic deal (market), the law, and code. To truly become a 'new architecture of trust', the governance of regulation of blockchain-based smart contracts would be shaped by all four forces. Importantly, these forces can be viewed as coexisting mechanisms in inducing trust between people and creating and sustaining commercial relations in a market economy.

Drawing from Lessig, one component may support or undermine another and changes in one will affect the regulation of the whole. For example, the precision and rigidity of code may make it extremely difficult for the 'real-deal' underpinning the transaction to be enforced. Parties would need to represent on smart contracts, *ex ante*, the 'real-deal' and all possible outcomes of the transaction. For many commercial transactions, this would be a challenging feat. It may also be undesirable considering the potential for undermining the long-term relationship of the parties. Let us take an example of a tenant who is five years into a 10-year commercial lease and unable to pay her rent on time due to changes in her business' financial circumstances. Based on the desire of both parties to maintain an ongoing relationship, the landlord may decide not to enforce the strict terms of the contract and instead, arrive at an arrangement with the tenant to allow for later payments. The landlord may even forego rent altogether for a few months. In many of these situations, the parties may choose to ignore a contractual breach for a variety of reasons, including the costs of requiring performance or enforcement, the desire to maintain goodwill and preserve the relationship (and even fortifying mutual trust).⁸⁹ A smart contract would not be able to offer parties such a choice.

If one takes into account the fuller picture of the real-world functions of contracts and contract law in market transactions as well as Levy's advice about 'thinking carefully about the features of the social setting in which smart contracts are permitted to operate',⁹⁰ then the 'rule of code' (*lex cryptographica*) will not replace other forces. It is likely that hybrid arrangements that link the substantive terms of a traditional contract with those of smart contract code will characterise the latter's development. Both books reviewed in this article have emphasised the possibilities of transposing legal agreements into code, whereby the agreements relying on smart contracts are legally enforceable.⁹¹ Like Collins, I suggest that the law can be seen as a remedial institution that functions as 'insurance' for parties to adjudicate grievances that may arise *ex post*, even when smart contracts have fully executed the agreement. The law will be used where and when it is useful.

5. Conclusion

As Werbach maintains, 'it would be premature to label the blockchain a revolution'.⁹² The *Blockchain and the Law* and *The New Architecture of Trust* have undertaken a meaningful analysis of this emerging technology and its potential regulatory, institutional, and social implications. An important question both books examine is how the 'regulatory architecture' of blockchain is likely to intersect with the law. Focusing on blockchain-based smart contracts, this article has sought to elucidate the need for an analytical framework which takes into account the role of norms, market, law, and code together in enabling a 'new architecture of trust' in commercial transactions.

⁸⁹ Zou, Heredia-Sorotia, Cheng (n 50).

⁹⁰ Levy (n 85) 11.

⁹¹ Werbach (n 5) 213; De Filippi & Wright (n 4) 76-77.

⁹² Werbach (n 5) 91.

Collins have suggested that for contract law to maintain its utility, it should be reconfigured to incorporate lessons from sociological and economic discourse of transacting in the marketplace.⁹³ In a similar vein, for smart contracts (and blockchain technology more generally) to realise their potential, we need to understand them as beyond mere ‘technical artefacts’ devoid of broader social and relational contexts. As Levy proposes, smart contracts should be viewed as ‘social resources’ that can be used by people to manage their relations, like traditional contracts.⁹⁴ Insights from this rich body of scholarship on relational analysis of contracting practices point to a potential future research direction that emphasise empirical studies of real-world ‘smart contracting’ in different domains of market transactions.

⁹³ Collins (n 81) 359.

⁹⁴ Levy (n 85) 2.