information

MDPI

Review

The Pervasiveness of Digital Identity: Surveying Themes, Trends, and Ontological Foundations

Matthew Comb * and Andrew Martin

Department of Computer Science, University of Oxford, Oxford OX1 3QD, UK; andrew.martin@cs.ox.ac.uk
* Correspondence: matthew.comb@cs.ox.ac.uk

Abstract

Digital identity operates as the connective infrastructure of the digital age, linking individuals, organisations, and devices into networks through which services, rights, and responsibilities are transacted. Despite this centrality, the field remains fragmented, with technical solutions, disciplinary perspectives, and regulatory approaches often developing in parallel without interoperability. This paper presents a systematic survey of digital identity research, drawing on a Scopus-indexed baseline corpus of 2551 publications spanning full years 2005–2024, complemented by a recent stratum of 1241 publications (2023–2025) used to surface contemporary thematic structure and inform the ontology-oriented synthesis. The survey contributes in three ways. First, it provides an integrated overview of the digital identity landscape, tracing influential and widely cited works, historical developments, and recent scholarship across technical, legal, organisational, and cultural domains. Second, it applies natural language processing and subject metadata to identify thematic patterns, disciplinary emphases, and influential authors, exposing trends and cross-field connections difficult to capture through manual review. Third, it consolidates recurring concepts and relationships into ontological fragments (illustrative concept maps and subgraphs) that surface candidate entities, processes, and contexts as signals for future formalisation and alignment of fragmented approaches. By clarifying how digital identity has been conceptualised and where gaps remain, the study provides a foundation for progress toward a universal digital identity that is coherent, interoperable, and socially inclusive.

Keywords: digital identity; interoperability; ontology; natural language processing; identity management; socio-technical systems; governance; privacy; security; trust

Academic Editor: Christoforos Kachris

Received: 7 December 2025
Revised: 3 January 2026
Accepted: 9 January 2026
Published: 13 January 2026

1. Introduction

1.1. Background and Motivation

The accelerating digitisation of modern life has made digital identity a foundational infrastructure for social participation, service delivery, and governance. As with the Internet itself—an asset that has transformed societies, but also enabled cybercrime and exploitation [1–3]—the design of identity systems introduces both opportunities and risks. Technical affordances such as encryption, VPNs, anonymity networks, and privacy-focused tools allow users to interact online without disclosing their true identities. While such mechanisms support freedom and innovation, they also facilitate identity theft, phishing, misinformation, and other forms of cybercrime [4].

To mitigate these risks, identity and access controls have become essential for authentication and authorisation [5]. Yet traditional username–password mechanisms are

increasingly insufficient, prompting a shift towards multifactor authentication, biometrics, and behavioural analytics [6]. At the same time, heightened awareness of privacy risks has driven the demand for systems that enable selective disclosure—asserting specific, verifiable claims (e.g., age, nationality, immunisation status, or credentials) without revealing the full identity of the subject. Cameron's Laws of Identity captured this shift, emphasising minimal disclosure and user control as guiding principles for modern identity frameworks [7].

Despite these advances, the domain of digital identity remains fragmented. Scholars such as Lyon [8] and others have highlighted the tension between benefits (fraud reduction, efficiency, inclusion, cross-border interoperability [9]) and concerns (privacy loss, surveillance, exclusion, lack of user control). Technically, persistent challenges remain: interoperability across platforms [10], privacy and data protection [11], resilience against cyber threats [5], usability trade-offs [12], compliance with diverse regulations [13,14], architectural scalability [15], heterogeneous network topologies [16], and long-term durability of identity infrastructures.

The consequence is a highly fragmented ecosystem of digital identity technologies, shaped independently by governments, industries, and social platforms, often with limited interoperability or shared conceptual grounding. This fragmentation underscores the need for a unifying perspective: one that is attentive both to the technical complexities and to the broader socio-ethical implications of identity in digital societies.

1.2. Scope and Objectives

Building on these societal and technical challenges, this survey is motivated by the broader aspiration of a universal digital identity: a conceptual and technical foundation that enables identity to function consistently and interoperably across domains, jurisdictions, and technologies. The goal is not to prescribe a single implementation, but to identify the underlying principles and conceptual structures that can bridge fragmented approaches, reduce risks of exclusion and surveillance, and support interoperability, inclusivity, and long-term trust.

Although "universal digital identity" is often invoked as a long-term aspiration, the more defensible and operational interpretation is interoperability: the ability for identity assertions and credentials to be recognised across heterogeneous technical stacks, governance models, and jurisdictions [7,17]. The benefits of interoperability as an integration goal are well documented, but so too are the practical barriers to achieving it in complex socio-technical environments (e.g., semantic heterogeneity, institutional fragmentation, and integration constraints) [18–20]. Accordingly, in this paper we treat an interoperable design as a minimum realisation of "universality," and we position ontological development as a necessary precursor because shared semantics are a prerequisite for interoperable protocols and conformance across ecosystems. Programmes such as eIDAS [21] provide a feasibility indicator for regulated cross-border interoperability within a defined governance regime, while also illustrating the challenge of integrating with identity ecosystems developed outside that jurisdiction and trust framework.

To contribute to this endeavour, the paper undertakes a comprehensive survey of digital identity research, drawing on Scopus-indexed publications where digital identity is a central theme. Unlike previous reviews that address specific technologies or isolated sectors, this study adopts a cross-disciplinary lens to capture the diversity of requirements and applications. It examines the evolution of digital identity through influential contributions, key developments, and recent scholarship, while systematically mapping thematic patterns, disciplinary trajectories, and leading authors.

The objective is therefore twofold: first, to provide researchers, policymakers, and system architects with an integrated map of the digital identity landscape; and second, to consolidate recurring concepts and relationships into a preliminary ontological foundation. By surfacing these structures, the study contributes to the longer-term goal of a universal digital identity: one that is conceptually coherent, technically interoperable, and ethically grounded.

1.3. Contributions of This Survey

This survey makes four primary contributions to the study of digital identity:

- Comprehensive Survey—This paper provides a systematic survey of nearly two decades of digital identity research, spanning influential contributions, historical developments, and the most recent three years of work. By mapping the field across technical, legal, organisational, and cultural domains, the survey offers a structured reference point for researchers, policymakers, and practitioners seeking an integrated understanding of how digital identity has evolved and is currently conceptualised.
- NLP-Supported Corpus Analysis—To achieve this breadth and consistency, the study constructs a targeted corpus of more than 2500 Scopus-indexed abstracts where digital identity is a central theme. Natural language processing techniques—including keyword extraction, clustering, and trend analysis—are applied to identify patterns that are difficult to observe through manual review alone. While not formalised as a general methodological framework, source code is provided and this computational approach strengthens the transparency and replicability of the survey.
- Key Authors and High-Impact Literature—The survey highlights the most influential works and leading authors across diverse fields—from computer science and law to sociology and public administration. This enables scholars to more easily identify the voices shaping the domain and the contributions that have had the most impact. By bringing together high-impact research across disciplinary boundaries, the study provides a valuable foundation for future work seeking to unify and systematise digital identity approaches.
- Ontological Groundwork—Finally, the paper consolidates recurring concepts and relationships into preliminary structures that support the development of a shared ontology of digital identity. Such groundwork encourages semantic alignment across disciplines and motivates subsequent ontology engineering; however, the present study does not claim a formal OWL/RDF ontology artefact and instead provides conceptually grounded fragments to guide future machine-readable modelling.

1.4. Structure of the Paper

The remainder of this paper is organised as follows. Section 2 reviews influential and widely cited works that have shaped the field of digital identity. Section 3 explains how the academic corpus was assembled and analysed, including the use of natural language processing to identify patterns and themes. Section 4 presents the results of this analysis, mapping influential literature, disciplinary distributions, and key authors across the field. Section 5 distils recurring concepts and terms into preliminary ontological structures that can serve as a foundation for future unification of digital identity approaches. Section 6 concludes by reflecting on the implications of the survey for researchers, policymakers, and system architects, highlighting opportunities for further study and practical application.

2. Notable Foundations in the Literature

This section offers a brief orientation to influential works in digital identity, illustrating key contributions that appear widely cited and enduring, to help position the present survey within the broader literature.

The evolution of digital identity reflects how technical, legal, and social contexts have shaped its meaning and practice over time. Westin's Privacy and Freedom (1967) defined privacy as control over personal information at a moment when governments and corporations were first automating records, setting the baseline for later digital identity debates [22]. In the context of growing computerisation, Chaum (1985) introduced cryptographic protocols for "security without identification," pioneering privacy-preserving credentials and pseudonyms to counter surveillance in electronic payments [23].

By the 1990s, identity was increasingly recognised as a socio-technical construct. In an era of expanding organisational databases, Clarke (1994) described the "digital persona" as the composite of data traces assembled by institutions [24]. Zuboff (1988) had already shown how workplace computing "informated" organisations, a critique Zuboff later extended in Surveillance Capitalism (2019) to highlight how platforms exploit personal data for behavioural prediction [25]. In parallel, the rise of the Internet enabled identity experimentation: Turkle (1995) examined how online users constructed multiple selves in virtual worlds, while boyd (2007) studied how youth on social media curated identity as a strategic performance shaped by peers, audiences, and surveillance [26,27].

The 2000s marked the institutionalisation of identity architectures. Cameron's Laws of Identity (2005) codified seven principles—including minimal disclosure and user control—at a time when federated login systems (e.g., Passport, Liberty Alliance) were proliferating [7]. In parallel, Cavoukian (1995; 2009) articulated Privacy by Design, embedding privacy into systems architecture, a principle later codified into the GDPR's Article 25 [28]. In Europe, Tóth (2004–2008), through FIDIS and PRIME projects, advanced privacy-enhancing identity management, emphasising proportionality and attribute-based credentials at a time of EU debates on biometrics and e-government [16]. Meanwhile, Solove (2004) framed digital identity in legal terms, warning in The Digital Person of risks from aggregation, secondary use, and data surveillance [29].

By the mid-2010s, identity systems were being embedded into law and infrastructure. The Electronic Identification, Authentication and Trust Services Regulation (eIDAS, 2014; revised 2024) created a European framework for cross-border electronic identification, while the General Data Protection Regulation (GDPR, 2016) reinforced privacy-by-design and rights-based safeguards [30]. At the same time, blockchain technologies revived Chaum's decentralisation ideals: Allen (2016) articulated the "Path to Self-Sovereign Identity," where individuals hold verifiable credentials in wallets—an approach now embedded in W3C DID and VC standards [31].

The evolution of digital identity—shaped by cryptographic foundations (Chaum, Allen), architectural and privacy frameworks (Cameron, Cavoukian), regulatory regimes (GDPR, eIDAS), and socio-cultural critiques (Clarke, Turkle, Boyd, Zuboff)—provides the spine of the field. Yet considerable contemporary research now turns to the detailed mechanisms, deployments, and implications of digital identity, and it is this ongoing work that forms the focus of the present study.

3. Methodology

3.1. Corpus Collection and Selection Criteria

This study draws upon a comprehensive corpus of scholarly literature on digital identity sourced from the Scopus Abstract and Citation Database. Scopus was selected because of its extensive interdisciplinary coverage, consistent metadata structure, and integration of citation and subject categorisation information—all of which are critical for downstream natural language processing and ontological analysis.

The corpus was assembled by querying for documents containing the exact phrase "digital identity" in the title, abstract, or author keywords fields. Notably, this retrieval query does not seed the corpus with blockchain- or ledger-specific terms; consequently, the prevalence of blockchain/ledger vocabulary in the results is interpreted as an emergent signal within the retrieved "digital identity" literature, rather than a direct artefact of search-term inclusion. Unlike approaches that limit analysis to specific document types, we retained all available document types, including journal articles, conference papers, book chapters, reviews, and short communications. This inclusive approach allowed for a broader view of the domain's discourse across scholarly genres.

To ensure conceptual relevance, we implemented a filtering step that combined automated keyword matching with Scopus-provided subject area classifications. Documents were retained if their abstracts demonstrated engagement with themes central to digital identity—such as authentication, identity management, privacy, trust, or decentralisation—as inferred from their keyword metadata and subject taxonomy. This process ensured the final corpus reflected meaningful participation in digital identity discourse, rather than incidental mentions of the term.

The resulting baseline corpus comprised 2551 publications spanning 2005 to 2024. In addition, a recent stratum comprising 1241 publications (2023–2025) was constructed to provide a contemporary thematic slice for detailed clustering interpretation and ontology-oriented synthesis.

We use article abstracts as the primary text unit for concept mining because abstracts are author-curated summaries that concentrate the central contributions and terminology of each paper, providing a relatively consistent and low-noise basis for large-scale analysis. Prior work notes that scientific text mining has often relied on abstracts due to their availability (e.g., not behind a paywall), whereas full-text access is frequently constrained and substantially increases preprocessing and computational overhead (e.g., file format conversion and boilerplate removal) [32,33]. For the objective of extracting high-level thematic structure and core concepts across a large corpus, comparative topic modelling evidence indicates that abstract-based models recover broad themes and that abstract–full-text differences become less pronounced as corpus size increases, with full text primarily contributing finer-grained detail in smaller collections [33]. At the same time, we acknowledge that full text can improve performance for some information extraction and retrieval settings [32,34,35]. Accordingly, and given the high level concept focus of this research, we interpret abstract-derived concepts as an efficient, reproducible approximation of the domain's core ideas, and we treat potential omission of technical detail as a limitation to be addressed in follow-on work through targeted full-text validation on accessible subsets.

Language Handling

Although Scopus indexes publications in multiple languages, the NLP pipeline in this study is English-centric and therefore operates on English-language abstracts. In practice, many non-English publications indexed by Scopus provide an English abstract; such records remain eligible for inclusion. Records without an English abstract are not meaningfully analysable under the present preprocessing and are therefore not represented in the

NLP-driven analyses. This choice supports methodological consistency and reproducibility, but introduces an English-dominant evidence base that may under-represent regionally situated scholarship published primarily in other languages.

3.2. Keyword Extraction and Preprocessing

To prepare the corpus for computational analysis, we first applied a structured preprocessing pipeline aimed at standardising the text and isolating meaningful lexical patterns. The focus of this stage was to ensure that downstream natural language processing (NLP) methods would operate on a semantically rich and noise-reduced representation of each abstract.

Each abstract was first tokenised and converted to lowercase to ensure uniformity. Standard stopwords (e.g., "the", "and", "of") were removed using the NLTK English stopword list, and all punctuation, numerals, and non-alphabetic characters were stripped. Words were then lemmatised using the WordNet lemmatiser to reduce inflected forms to their root form, thereby consolidating semantically equivalent terms (e.g., "identities" $\rightarrow$ "identity"). These preprocessing steps assume English text (e.g., English stopwords and WordNet-based lemmatisation) and are therefore applied to English-language abstracts.

In parallel, we extracted author-supplied keywords provided through Scopus metadata for each publication. These keywords were normalised using the same preprocessing steps and incorporated as weighted lexical features to augment the representation of domain-specific concepts that may be under-represented in the abstract text. For example, specialised terms such as "self-sovereign identity" or "verifiable credential"—while critical to the digital identity domain—may appear only once or be paraphrased in the abstract body. Their presence in the author keyword list provided valuable anchoring for cluster relevance.

A custom keyword harmonisation step was introduced to reduce fragmentation in concept representations across the corpus. Harmonisation followed a defined protocol. First, orthographic variants were unified (e.g., British/American spellings; hyphenation such as *block-chain* vs. *blockchain*). Second, singular/plural and minor morphological variants were consolidated where semantic meaning is preserved. Third, common abbreviations and expanded forms were mapped to a canonical term where usage is unambiguous within the domain. Fourth, near-synonyms were merged only when terms are routinely used interchangeably in the literature and the merge does not collapse materially distinct constructs; where ambiguity remained, terms were preserved as distinct rather than forced into a single label.

To reduce subjectivity and improve consistency using a single-reviewer workflow, we applied two validation steps. First, we performed automated consistency checks on the mapping dictionary, including idempotency (i.e., repeated application yields a stable canonical form) and collision detection to flag cases where many-to-one merges could collapse distinct high-frequency concepts. Second, we conducted an intra-annotator test–retest reliability check by repeating harmonisation decisions for a stratified sample of 50 mappings after a 14 day interval and quantified agreement between passes using *Cohen's* κ. Conflicts were adjudicated conservatively; where a merge risked conceptual collapse, distinct terms were retained.

The result of this process was a clean, lemmatised, and semantically consolidated corpus, suitable for vectorisation and clustering. This preparatory step was essential for capturing consistent themes and identifying emergent patterns across the digital identity research landscape.

3.3. NLP Techniques and Vectorisation

To prepare the corpus for semantic analysis, we extracted keywords from titles and abstracts, and applied standard NLP techniques, including tokenisation, lowercasing, and stopword removal. The processed corpus was then vectorised using term frequency (TF), document frequency (DF), and TF-IDF representations to support both statistical and semantic analysis.

For embedding-based analysis, we trained domain-specific word embeddings using the Word2Vec algorithm. A vector dimension of 100 and context window size of 5 were selected to balance semantic expressiveness and training stability, following best practices for medium-sized academic corpora. The resulting embeddings file was used as input to clustering and ontological framing tasks.

3.4. Clustering and Coherence Evaluation

Clustering was used to identify latent thematic groupings within the digital identity literature. In this study, clustering is performed at the level of *terms/concepts* by applying unsupervised clustering to Word2Vec term-embedding vectors derived from the corpus vocabulary. This design choice aligns with the paper's objective of extracting an interpretable thematic structure of the domain's core concepts and supporting subsequent ontology-oriented synthesis.

1. Clustering Method—K-Means clustering was applied to the Word2Vec *term* vectors to partition the corpus vocabulary into groups of semantically related concepts. We cluster terms (rather than documents) because the analysis is intended to recover domain-level conceptual structure: term clusters yield compact, interpretable keyword sets that support thematic labelling and concept/ontology mapping. In contrast, document embeddings would often blend multiple themes within a single paper and would require forcing multi-topic articles into single partitions, which is less aligned with the study's ontology-oriented emphasis. To connect term clusters back to the literature for interpretation, we examine representative titles/abstracts associated with salient cluster terms and use these exemplars to characterise each cluster's substantive focus.
2. Cluster Number—The determination of the optimal number of clusters was guided by coherence testing. We evaluated inertia (within-cluster sum of squares), silhouette score (inter-cluster separation), and the interpretability of the top terms in each cluster. This combined assessment followed an explicit quantitative-primary weighting. Inertia and silhouette were used as the primary diagnostics to identify the best-performing (or near-best-performing) range of candidate k values. Qualitative interpretability checks (coherence and distinctiveness of the top-term lists, and clarity of cluster characterisation during labelling) were then applied only as a tie-breaker when multiple k values were quantitatively comparable or when differences in metrics were not practically meaningful. In those cases, we preferred the k that yielded the most coherent and least redundant top-term sets and supported clear thematic interpretation.
3. Cluster Labelling—Each cluster was then labelled using the top 20 high-weight terms identified through TF–IDF analysis. These keyword sets were supplied to the OpenAI API with prompts designed to generate concise thematic labels that abstracted and generalised the terms while avoiding overlap. Human review was subsequently applied to refine the labels and ensure they accurately represented the semantic content of the clusters.
4. Evaluation of Label Accuracy—To validate the accuracy of the generated labels, we assessed cluster coherence through several steps. These included inspecting intra-cluster term homogeneity, cross-checking cluster contents against representative

document titles and abstracts, and verifying alignment with known domains of digital identity such as technology, law, governance, and user experience. This process ensured the assigned labels faithfully captured the substantive themes of the clusters and also informed the framing of a draft ontology.

5. Stability and Reliability—To assess the reliability of the unsupervised solution under random initialisation, we reran K-Means across multiple random seeds and initialisations and compared the resulting partitions for agreement. Agreement was assessed using standard assignment-comparison diagnostics (e.g., adjusted Rand-style indices) alongside overlap of top-weight terms within each cluster. This procedure provides a robustness check that cluster boundaries and thematic interpretations are not artefacts of a single initialisation.

3.5. From Computational Themes to Ontological Structures

The ontological framing in this study is derived from empirical regularities in the corpus rather than introduced as an independent conceptual model. Specifically, the clustering outputs and recurrent keyword distributions are used as ontological signals to identify candidate concepts and stable thematic strata across the literature. The cluster keyword sets (Tables 1 and 2) provide empirically grounded concept groupings, while the cluster-set comparison (Table 3) highlights which groupings persist, split, or consolidate over time.

We operationalise this linkage in three steps. First, we treat the normalised corpus vocabulary (including harmonised author keywords) as a pool of candidate concepts and prioritise terms that are both frequent and structurally informative within clusters (e.g., those anchoring distinctive cluster themes or appearing across multiple clusters). Second, we interpret cluster structure as evidence of higher-level conceptual strata in the domain—most visibly, a technical "rails" layer (architectures, credentials, security/privacy controls), a governance/institutional layer (policy, standards, programmes), and a use-and-practice layer (sectoral adoption and socio-cultural settings).

Table 1. Clusters and Associated Keywords in the 2005–2024 Digital Identity Corpus.

#	Cluster	Associated Keywords
1	Digital Identity Applications and Emerging Tech.	applications, blockchain, education, health, healthcare, implications, industry, potential, profiling, safety, security, smart, technology, trends, usability
2	Identity Architectures and Trust Frameworks	application, architecture, authentication, centralised, credentials, decentralised, decentralized, design, digital, enabled, federation, framework, identity, implementation, model, platform, private, revocation, service, sovereign, systematic, unlinkability, verifiable, wallet
3	Privacy, Rights, and Risk Management	anonymity, confidentiality, information, knowledge, legal, personal, privacy, protection, rights, risks, users
4	Cyber Environments and Emerging Digital Ecosystems	behavior, cloud, communication, communications, computer, computing, construction, cyber, distributed, environment, environments, generation, human, humans, intelligence, internet, learning, metaverse, metaverses, network, networks, power, virtual, world
5	Biometric Identification Technologies	access, biometric, biometrics, fingerprint, identification, system, systems, technologies
6	Identity Management, ACL, and Trust Services	authorization, control, electronic, identities, management, managing, offline, online, preserving, secure, services, trust
7	Societal and Cultural Digital Identity Dimensions	academic, covid, culture, digitisation, educational, facebook, female, gender, instagram, literacy, male, media, networking, people, practice, practices, professional, school, social, spanish, students, survey, teachers, theory, twitter, university
8	Cluster 8 Governance, Policy, Standards, and Regulations	aadhaar, adoption, australia, building, business, consumer, development, economy, ecosystem, eidas, european, evolution, financial, future, global, governance, government, inclusion, india, international, introduction, national, policy, public, regulation, regulatory, scientific, society, technological, transformation

Table 2. Clusters and Associated Keywords in Recent Years 2023–2025.

#	Cluster	Associated Keywords
1	Credentials, Wallets, and Trust Services	access, authentication, centralised, contracts, credentials, information, private, public, revocation, service, unlinkability, verifiable, wallets
2	Enterprise Adoption and Immersive/Global Contexts	adoption, applications, business, corporate, cybersecurity, digitalization, environments, financial, future, governance, human, immersive, intelligence, international, management, metaverse, metaverses, opportunities, potential, regulatory, solutions, technology, transformation, trends, virtual, world
3	Methodologies, Models, and Assurance Workflows	adulteration, application, comparative, design, enhancing, learning, method, model, modeling, models, multi, processes, smart, system, systematic, traceability, usability, verification
4	Security, Privacy, and Data-Protection Foundations	computing, internet, knowledge, networks, preserving, privacy, protection, rights, security, theft, trust
5	Decentralised Identity and Persona/Presentation	authenticity, avatar, decentralised, decentralized, digital, humans, identities, identity, personal, platform, platforms, presentation, secure, sovereign, systems, users
6	Socio-Cultural and Educational Practices Online	behavior, borders, chinese, community, construction, consumer, culture, dynamics, educational, engagement, female, gender, influence, instagram, language, literacy, media, online, personality, power, practice, practices, professional, representation, sharenting, social, spaces, students, survey, teacher, teachers, theory, understanding, university, youth
7	Governance, Policy, and European Frameworks	border, ecosystem, eidas, electronic, european, framework, gdpr, government, identification, implementation, indonesia, legal, mobility, national, policy, regulation, wallet
8	Sectoral Innovations and Public-Interest Applications	artificial, blockchain, cities, communication, education, energy, global, health, healthcare, india, intelligent, safety, sustainable, technologies

Table 3. Mapping of corpus-wide clusters (2005–2024) to recent clusters (2023–2025).

2005–2024 Cluster	Nearest 2023–2025 Counterpart (s)	Change Note
Identity Architecture & Trust Frameworks	Credentials, Wallets & Trust Services; Decentralised Identity & Persona/Presentation	Splits into operational wallet/VC rails vs. decentralised/persona layer across platforms.
Identity Mgmt., Access Control & Trust Services	Credentials, Wallets & Trust Services	Largely absorbed into wallet-centric operational focus (status, revocation, unlinkability).
Privacy, Rights & Risk	Security, Privacy & Data-Protection Foundations	Substantive continuity with consolidation around networked/data-protection concerns.
Governance, Policy, Standards & Regulation	Governance, Policy & European Frameworks	Continuity with enhanced eIDAS/GDPR/wallet framing and implementation guidance.
Applied Use-Cases & Emerging Tech	Sectoral Innovations & Public-Interest Applications; Enterprise Adoption & Immersive/Global Contexts	Broadens into sector pilots/scale-ups (health, education, cities/energy) and enterprise/immersive adoptions.
Cyber Infrastructures & Digital Ecosystems	Enterprise Adoption & Immersive/Global Contexts; Sectoral Innovations; Security/Privacy Foundations	Recontextualised: ecosystem view diffuses into specific domains plus firmer security baseline.
Social, Educational & Cultural Contexts	Socio-Cultural & Educational Practices Online	Continuous, with richer platform/youth practices (e.g., Instagram, sharenting).
Biometrics & Identity Proofing	(Distributed across Methods/Assurance; Wallet/Credential; Sectoral deployments)	No longer a standalone focal cluster; concerns appear within assurance flows and deployments.

Third, to support interpretability, we visualise selected "core terms" that recur across the recent thematic structure (e.g., credentials, security, system, blockchain, society) as subgraphs (Figures 1–5). Nodes represent candidate concepts that co-occur with, or are semantically associated with, the core term within the recent literature stratum; edges summarise salient associations as indicative relationships to aid conceptual interpretation. These visualisations are intended as preliminary scaffolding to motivate future formalisation (e.g., typed relations and constraint definitions), and they are therefore interpreted as empirically grounded concept maps rather than a complete or normative ontology.

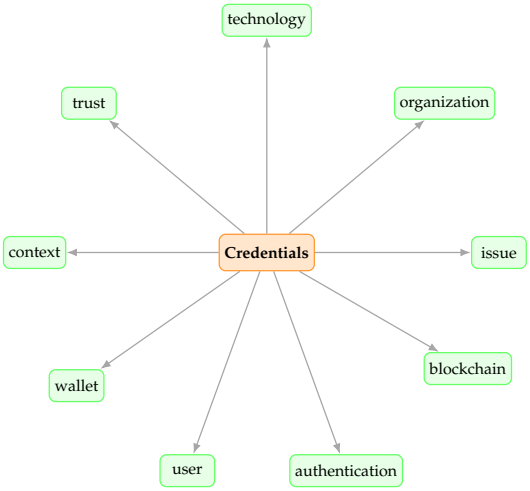

Figure 1. Credential subgraph of the digital-identity ontology (2023–2025)—derived from the recent thematic structure and intended as an illustrative, empirically grounded concept map.

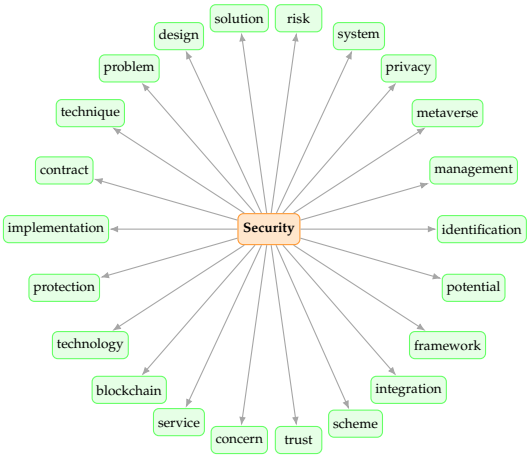

Figure 2. Security subgraph of the digital-identity ontology (2023–2025)—derived from the recent thematic structure and intended as an illustrative, empirically grounded concept map.

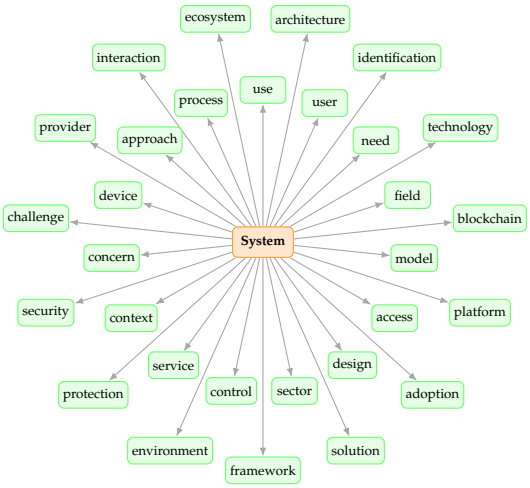

Figure 3. System subgraph of the digital-identity ontology (2023–2025)—derived from the recent thematic structure and intended as an illustrative, empirically grounded concept map.

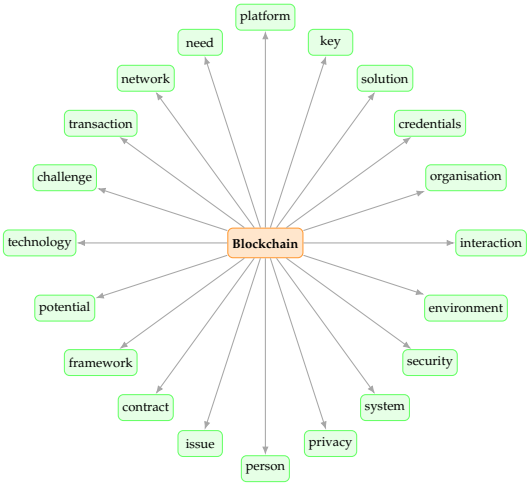

Figure 4. Blockchain subgraph of the digital-identity ontology (2023–2025)—derived from the recent thematic structure and intended as an illustrative, empirically grounded concept map.

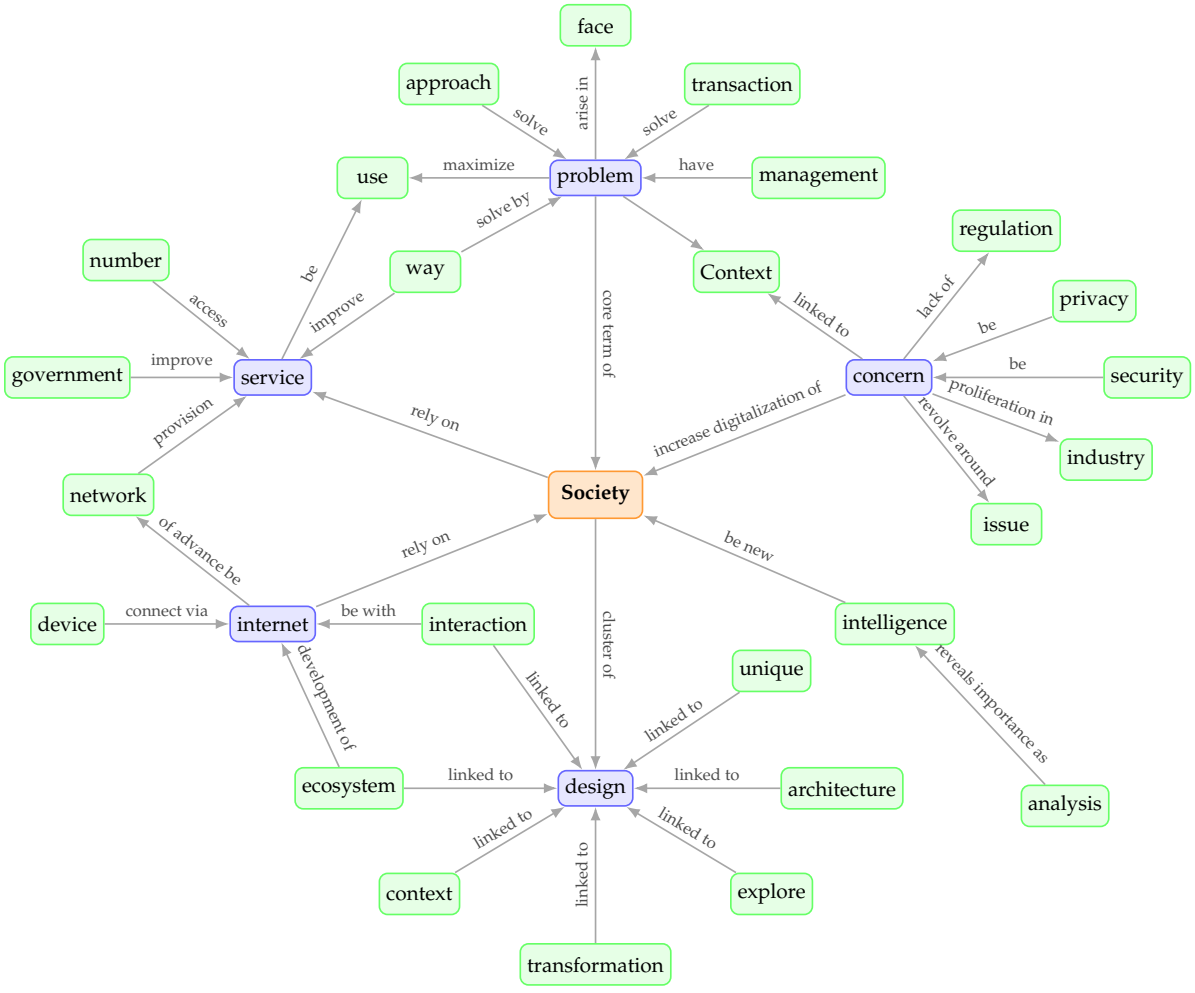

Figure 5. Society subgraph of the digital-identity ontology (2023–2025).

Conceptual Boundaries

Digital identity spans legal, social, and technical constructs, creating a risk of category leakage if concepts are treated as undifferentiated vocabulary. To mitigate this, we apply explicit boundary conditions when interpreting computational outputs. Concepts are treated as within-scope when they (i) directly support digital identity system functions (e.g., identification, authentication, authorisation, credential issuance/presentation/verification, life-

cycle events such as recovery and revocation, or assurance and auditability mechanisms), or (ii) materially constrain or shape deployment contexts (e.g., regulatory frameworks, institutional trust arrangements, user agency and accessibility constraints, or sector-specific service delivery requirements). Concepts that are primarily about identity in general (without clear linkage to digital identity systems, infrastructures, or governance contexts) are treated as out-of-scope for ontological synthesis even if they appear in the corpus. We operationalise separation using the three-strata framing (technical rails; governance and institutions; use and practice) as an interpretive structure that maintains analytic distinctions while permitting controlled overlap: where concepts genuinely span strata (e.g., trust, privacy, accountability), they are treated as cross-cutting rather than forced into a single category.

4. Corpus Composition

In this section, we present this study's corpus at a glance—its overall size, time span, document types, venues, and topical makeup. The aim is to give a clear picture of what is in scope before turning to patterns within it.

4.1. Descriptive Statistics

The baseline corpus comprises 2551 distinct articles authored by 2030 distinct researchers, spanning 188 subject areas and 8820 distinct keywords. A separate recent stratum (2023–2025; n = 1241) is analysed in Section 7 to characterise contemporary themes and support the ontology-oriented subgraphs. Authorship, presented in Table 4, is broad rather than concentrated ($\tilde{1}$.26 articles per author on average), and the topical footprint is wide, indicating coverage across policy, technical architectures, and applied domains. The lexical scope ($\tilde{3}$.46 distinct keywords per article) reflects the field's many use cases—ranging from authentication and privacy to governance, compliance, and sectoral deployments in areas such as finance, health, public services, and connected devices. Overall, these figures characterise a large, diverse literature well suited to subject-level, temporal, and semantic analyses of digital identity and its applications.

Table 4. Top 20 Authors—Articles & Four Most Frequent Subjects.

Author	Articles	Subjects			
Bertino E.	27	Computer Networks and Comms 13	Software 13	Computer Science 9	Engineering 4
Sullivan C.	15	Business, Management and Accounting 8	Computer Networks and Comms 8	Law 8	Public Administration 2
Buccafurri F.	13	Computer Science 6	Computer Networks and Comms 4	Computer Science Applications 4	Theoretical Computer Science 4
Liu Y.	13	Computer Networks and Comms 9	Hardware and Architecture 4	Information Systems 3	Computer Science 2
Wang Y.	12	Computer Science Applications 7	Artificial Intelligence 3	Computer Graphics and CAD 3	Computer Networks and Comms 3
Meinel C.	12	Computer Networks and Comms 4	Computer Science Applications 4	Information Systems and Management 4	Engineering 3
Zhang J.	11	Computer Networks and Comms 4	Information Systems 3	Artificial Intelligence 2	Computer Graphics and CAD 2
Lax G.	11	Computer Networks and Comms 4	Computer Science 4	Computer Science Applications 3	Software 3
Carbone R.	11	Computer Science 6	Theoretical Computer Science 5	Computer Networks and Comms 4	Software 3
Ranise S.	11	Computer Science 6	Theoretical Computer Science 5	Computer Networks and Comms 4	Software 3
Wang X.	10	Computer Networks and Comms 3	Electrical and Electronic Engineering 3	Computer Science 2	Computer Science Applications 2
Naik N.	10	Computer Networks and Comms 6	Computer Science Applications 6	Control and Systems Engineering 5	Hardware and Architecture 5
Jenkins P.	10	Computer Networks and Comms 6	Computer Science Applications 6	Control and Systems Engineering 5	Hardware and Architecture 5

Table 4. *Cont.*

Author	Articles	Subjects			
Squicciarini A.C.	10	Software (5)	Computer Networks and Comms (4)	Computer Science (3)	Safety, Risk, Reliability and Quality (2)
Li M.	9	Artificial Intelligence (2)	Computer Networks and Comms (2)	Computer Science Applications (2)	Chemistry (1)
Li J.	9	Computer Networks and Comms (6)	Computer Science Applications (4)	Artificial Intelligence (3)	Information Systems and Management (3)
Bhargav–Spantzel A.	9	Software (4)	Computer Networks and Comms (4)	Computer Science (3)	Theoretical Computer Science (2)
Sedlmeir J.	8	Information Systems (4)	Computer Science Applications (3)	Behavioural Neuroscience (1)	Business and International Mgmt (1)
Fridgen G.	8	Information Systems (2)	Behavioural Neuroscience (1)	Computer Networks and Comms (1)	Computer Science (1)
Pohn D.	8	Engineering (4)	Computer Science (3)	Materials Science (3)	Computer Science Applications (2)

Citation totals (see Table 5) are reported as a cumulative indicator of scholarly uptake, but they are inherently time-dependent and therefore favour older publications with longer citation windows. We interpret these summaries as signals of *historical influence* rather than recency-adjusted impact. While year-normalised measures (e.g., citations/year) can reduce age effects, they are sensitive to citation latency, indexing delays, and publishing seasonality—particularly over short windows—so we avoid presenting per-year citation visualisations as a primary result. Instead, we complement long-run citation signals with a dedicated contemporary stratum (2023–2025) to surface recent thematic emphases that may not yet be reflected in mature citation accumulation.

Table 5. Top 20 Authors by Citation Count.

Author	Citations
Arner D.W.	831
Eller R.	534
Sullivan C.	350
Dunphy P.	345
Naik N.	335
Bouncken R.B.	327
Adat V.	294
Brubaker J.R.	278
Zhu X.	276
Efanov D.	267
Rouhani S.	253
Liu Y.	252
Veletsianos G.	239
Sarma A.C.	216
Soltani R.	182
Maler E.	178
Vargas A.O.	176
Josang A.	175
Hosseini Bamakan S.M.	170
Martzoukou K.	164

4.2. Keyword Analysis

Table 6 enumerates term frequencies from a digital-identity corpus in descending order, revealing a concentration of signal in a small set of high-salience items—most notably digital identity, followed by foundational tokens such as digital and identity.

Table 6. Top keywords and counts.

Term	Count
digital identity	915
digital	493
identity	476
block-chain	427
identity management	239
decentralised	161
security	140
privacy	130
digital identity management	125
self-sovereign identity	115
identity management systems	99
social	88
management	88
identities	77
media	59
privacy preserving	56
technology	55
online	53
trust	52
cyber security	50
humans	49
social media	48
systems	48
international	48
internet	44
service provider	44
verifiable credential	43
information	41
centralised	39

Apparent near-duplicates in the table therefore often reflect deliberate preservation of conceptual granularity for highly central terms (where small lexical differences encode materially different constructs), rather than incomplete lemmatisation. Beyond these anchors, the vocabulary foregrounds several thematic blocks. Security and trust feature prominently, with security, privacy, privacy preserving, trust and cyber security indicating sustained attention to protection, assurance and risk. Architectural and governance concerns appear through decentralised, centralised and service provider, reflecting debates on control models, infrastructure and intermediary roles.

Self-sovereign identity and credentialing are visible via self-sovereign identity and verifiable credential, while operational and organisational layers surface in identity management, digital identity management, identity management systems, systems and information. A broader socio-technical context is suggested by social, media, social media, humans, international, internet and technology, situating identity work within platforms, actors and settings. The frequency profile is steep—declining from several hundred to a few dozen—consistent with a long-tail distribution in which a handful of dominant terms frame the discourse while mid-frequency items articulate key subtopics.

Computation

Counts in Table 6 are document-frequency-style tallies: for each term or multi-word expression, we count the number of corpus records whose processed abstract and/or author keywords contain the term after the preprocessing and harmonisation pipeline in Section 3.2 The table therefore reflects how widely a concept appears across publications (presence/absence per record), rather than within-document token frequency.

4.3. Subject Analysis

Table 7 summarises subject-area coverage within the digital-identity corpus, listing fields by article count. Scopus subject areas are non-exclusive: a single publication may be assigned to multiple subject labels. Accordingly, the counts in Table 5 should be interpreted as *presence* within a subject area rather than a partition of the corpus into mutually exclusive disciplines. This overlap is expected in a socio-technical domain such as digital identity and provides an additional signal of interdisciplinarity rather than a classification error. Technical domains predominate: Computer Networks and Comms leads, followed by Computer Science and Computer Science Applications, with substantial representation from Information Systems and Artificial Intelligence. Applied and infrastructural areas—Software, Information Systems and Management, Hardware and Architecture, Electrical and Electronic Engineering, and Computer Vision and Pattern Recognition—underscore an implementation-oriented emphasis. Human- and organisation-centred strands appear through Education, Human–Computer Interaction, Social Sciences, and Sociology and Political Science, indicating attention to adoption, usability, and societal effects. Governance and market interfaces are visible via Business, Management and Accounting, Law, and Economics, Econometrics and Finance. Sectoral and methodological niches—Health Informatics, Control and Systems Engineering, Signal Processing, and Control and Optimisation—round out the landscape. Overall, the distribution is skewed towards core computing fields, but exhibits meaningful breadth across managerial, legal, and social perspectives, consistent with the multi-stakeholder nature of digital identity.

Table 7. Subject areas and article counts.

Subject Area	Articles
Computer Networks and Comms	748
Computer Science	504
Computer Science Applications	489
Information Systems	347
Artificial Intelligence	300
Software	293
Information Systems and Management	272
Social Sciences	216
Safety, Risk, Reliability and Quality	175
Hardware and Architecture	169
Electrical and Electronic Engineering	168
Computer Vision and Pattern Recognition	166
Education	163
Human-Computer Interaction	159
Engineering	158
Business, Management and Accounting	136
Theoretical Computer Science	130
Communication	124
Law	120
Economics, Econometrics and Finance	119
Control and Systems Engineering	109
Signal Processing	103
Sociology and Political Science	94
Health Informatics	70
Control and Optimisation	67

5. Influential Literature by Subject

This section presents the most cited digital identity articles within each subject area (with more than five citations), organised using Scopus' primary subject classification for

readability. Because Scopus subject labels are multi-assigned, many articles span multiple areas; the groupings therefore indicate the dominant indexing category rather than a claim of disciplinary exclusivity. The aim is to highlight leading contributions and illustrate the disciplinary diversity of the field. Because citation counts are cumulative and time-dependent, the selections in this section should be read as historically influential within each subject area; contemporary emphases are examined separately in the 2023–2025 stratum.

These subject-area exemplars are selected by citation count to illustrate disciplinary diversity and historically influential contributions within each Scopus indexing category. They are not selected to be representative of the most prominent corpus-wide themes, and they are not expected to map consistently to the NLP-derived clusters, which are computed at the term/concept level to recover cross-disciplinary thematic structure. Accordingly, this should be read as complementary to the thematic cluster analysis which characterises the dominant concept groupings across the full corpus and the recent stratum.

5.1. Biochemistry, Genetics and Molecular Biology

In the life sciences, digital identity is treated as portable, attribute-based access to sensitive data. Voisin et al.'s GA4GH Passport encodes these rights as machine-readable "visas" aligned with consent and ethics approvals; deployments across ELIXIR, NIH, and the Autism Sharing Initiative demonstrate secure, federated, cross-border sharing with improved transparency and reproducibility [36] (17 citations).

5.2. Business and International Management

In international management, digital identity functions as market infrastructure for cross-border trust, compliance, and coordination. Efanov and Roschin frame blockchain's evolution (1.0 to 3.0) as lowering transaction costs and widening inclusion via identity while flagging privacy, scalability, and interoperability risks [37]. At the company level, Bouncken and Barwinski show that a shared digital identity underpins knowledge exchange and boundary-spanning collaboration in global 3D-printing networks [38]. Translating these logics into finance and trade, Takemiya and Vanieiev's Sora Identity and Naik and Jenkins' SSI principles enable portable, privacy-preserving credentials aligned with KYC/AML [39,40]. In parallel, Arner et al. chart the rise of digital KYC utilities (Aadhaar, GovPass, eIDAS) that reduce compliance costs and expand SME access [41]. Together, these contributions highlight digital identity as both an enabler of new global business models and a mechanism to address critical challenges of trust, compliance, and collaboration in international management.

5.3. Business, Management and Accounting

Across this closely related subject area, digital identity operates as both a technical coordination layer and a socio-institutional mechanism that structures trust, behaviour, and legitimacy in distributed markets. Zhu and Badr survey blockchain-based IoT identity (Namecoin, Certcoin, uPort, Sovrin), arguing that user-controlled, decentralised credentials better satisfy scalability, interoperability, and privacy requirements while lowering assurance and transaction costs in supply chains [42]. In entrepreneurial finance, Block et al. show that venture capital funding reshapes entrepreneurs' digital self-presentation—enhancing professionalism and self-efficacy while attenuating authenticity—with effects moderated by investor reputation and deal size [43]. Additionally, in platform labour markets, Hondros et al. demonstrate that workers assemble collective identity infrastructures (e.g., FAWM, MTurk) to sustain belonging, legitimacy, and coordinated action amid platform transience [44] (6 citations).

5.4. Communication

Across the communication subdomain, research shows how digital identity functions as a site of negotiation between self-presentation, inequality, activism, and design. Kavakci and Kraeplin demonstrate how hijabi social media influencers ("hijabistas") merge modesty with fashion, producing hybrid identities that balance religious norms, audience expectations, and marketable branding within the attention economy [45]. Robinson extends this lens to the online practices of youths, framing identity curation as a "game" that demands constant updating, reciprocal validation, and vigilance. In this context, high-connectivity youths set normative standards, while those with limited access face exclusion and negative emotions, showing how unequal digital resources shape both identity work and emotion management [46]. Vivienne highlights the activist potential of digital identity, arguing that online self-representation operates simultaneously as personal narrative and public message, enabling resistance, community building, and everyday political participation [47]. Complementing these perspectives, Manas-Viniegra et al. provide empirical evidence that visual design influences identity recognition: young audiences respond more positively to flat, minimalistic logos than to 3D designs, illustrating how digital aesthetics strengthen identity through improved recognition, modernity, and platform fit [48].

Combined, these studies reveal communication as a subject area where digital identity is shaped not only by personal agency, but also by external conditions—including cultural values, digital inequalities, political engagement, and design affordances. The overarching narrative is that communication research demonstrates digital identity as a multi-layered construct that both reflects and reshapes how individuals and groups negotiate visibility, belonging, and influence within digital environments.

5.5. Computer Graphics and CAD

In the computer graphics and CAD subdomain, digital identity research emphasises the critical role of interoperability in enabling secure collaboration across heterogeneous platforms. Ates et al. analyse identity federation architectures, focusing on SAML 2.0 and WS-Federation 1.1B, and propose a third-party mechanism capable of translating requests and responses [49]. Their study demonstrates how technical standards for identity interoperability are foundational to ensuring reliable access management in complex, multi-system environments.

5.6. Networks and Communications

Within the area of networks and communications, research highlights how digital identity technologies underpin secure, trustworthy, and scalable interactions across distributed environments. Lee introduces BIDaaS, a blockchain-based identity-as-a-service model that manages virtual IDs through private blockchains to enable mutual authentication without the need for new accounts or partner-held sensitive data [50]. This illustrates how blockchain architectures can streamline identity exchange, reduce overhead, and strengthen trust across interconnected digital services. Schanzenbach et al. extend this trajectory through reclaimID, a decentralised self-sovereign identity system that leverages name systems and attribute-based encryption to give users control over sharing and revoking attributes [51]. Their work demonstrates how decentralisation can enhance privacy and scalability while reducing dependence on centralised authorities.

Cocco et al. apply these principles to supply chains, combining blockchain, self-sovereign identity, and IPFS to manage food certifications [52]. Their system illustrates how decentralised identity enables transparency, interoperability, and compliance across distributed networks. Complementing this, Naik and Jenkins examine identity and access management in mobile cloud computing, arguing that existing standards such as LDAP,

SAML, OAuth, and OIDC are insufficient for mobile contexts [53]. They call for lightweight, scalable, and user-friendly IAM models tailored to mobile environments, where security and interoperability are especially critical. More recently, Zhang et al. proposed IDRG, a system that integrates identity-based encryption with redactable blockchains to govern access and editing rights in the metaverse [54]. Their work highlights how identity can enable flexible and privacy-preserving data governance in emerging human-centric communication spaces.

Taken together, these studies illustrate how digital identity in networks and communications is central to building secure, interoperable, and trustworthy infrastructures. From blockchain-based authentication to decentralised attribute management, supply chain traceability, mobile IAM, and metaverse data governance, the overarching narrative emphasises identity as a foundation for enabling trust, flexibility, and resilience across increasingly complex and distributed digital ecosystems.

5.7. Computer Science

In the broad area of computer science, digital identity research examines both the technical architectures that enable secure interaction and the socio-ethical implications of identity construction. Beck highlights how cookies, flash cookies, and web beacons assemble "invisible digital identities" by harvesting and selling user data, shaping online behaviour, and raising significant privacy concerns. Beck frames algorithms as active agents in the construction of identity, underscoring the need for transparency and digital literacy in algorithmic systems [55]. Goodell and Aste propose a decentralised digital identity architecture using distributed ledgers and blind signatures, which allows individuals to manage multiple, unlinkable identities. Their design reduces dependence on central authorities, resists surveillance, and emphasises privacy and autonomy in digital interactions [56].

Schoemaker et al. examine the lived experiences of refugees navigating digital identity systems in Lebanon, Jordan, and Uganda. They show how opaque registration processes undermine user agency, even as credentials remain essential for accessing services. Using a data justice framework, they argue that humanitarian identity infrastructures often reinforce inequality and call for participatory, feminist-informed approaches that uphold refugee dignity [57]. Complementing this focus on social justice, Paci et al. address the technical challenge of naming heterogeneity by developing a multifactor verification protocol. Their model combines lookup tables, ontology mapping, and ZKPs to enable secure, privacy-preserving identity verification across heterogeneous systems [58]. Munoz-Rodriguez et al. add a further perspective by exploring digital identity in the context of older adults. They propose a three-level model—location, action, and significance—validated through a study of 659 senior learners in Spain, showing how online practices and even social isolation can contribute to stronger digital identities that support lifelong learning and active ageing [59].

Taken together, these studies illustrate how digital identity research in computer science spans both infrastructural and human-centred concerns. From privacy risks in algorithmic tracking to decentralised architectures, from refugee experiences to semantic interoperability, and from older adult inclusion to lifelong learning, the overarching narrative is that digital identity in computer science operates at the socio-technical intersection of innovation and impact.

5.8. Computer Science Applications

In computer science applications, blockchain emerges as a central theme in the reconfiguration of digital identity management. Lim et al. survey systems such as Sovrin, uPort, ShoCard, and Bloom, arguing that blockchain enables self-sovereign, tamper-proof identities, but noting that challenges in scalability, governance, and integration limit widespread

adoption [60]. Zwitter et al. similarly emphasise blockchain's transformative potential, framing digital identity as a universal infrastructural service enabled through distributed ledgers and ZKPs. Drawing on case studies from Estonia, the Netherlands, and humanitarian contexts, they highlight both the promise of autonomy and inclusion, as well as risks of surveillance and weak governance, underscoring the importance of legal and ethical safeguards [61].

Rathee and Singh provide a systematic review of 30 blockchain-based identity management initiatives from 2009 to 2020, including Sovrin, uPort, and several EU-funded projects. They conclude that while blockchain addresses challenges of security, privacy, anonymity, trust, and interoperability, significant barriers remain in scalability, interoperability, privacy protection, and key management [62]. Grech et al. extend this discussion to the education sector, demonstrating how blockchain, self-sovereign identity, and digital credentials can support secure, portable, and user-controlled records. They argue that while decentralised identifiers (DIDs) and verifiable credentials offer technical potential, widespread adoption depends on addressing governance, interoperability, and trust issues [63].

Together, these studies reveal blockchain as both an enabler and a challenge in computer science applications of digital identity. While decentralisation, tamper-resistance, and self-sovereignty provide a compelling vision of user-controlled identity, unresolved questions around scalability, interoperability, governance, and ethics demonstrate that technical innovation must be integrated with institutional and regulatory frameworks to achieve sustainable adoption.

5.9. Control and Systems Engineering

In the control and systems engineering subdomain, digital identity research addresses the security and resilience of cyber-physical systems. Mamun et al. propose a blockchain-based identity framework that replaces centralised authentication with decentralised ledgers and smart contracts, thereby reducing vulnerabilities and improving trust [64]. Their approach demonstrates how decentralised identity infrastructures can strengthen the reliability and resilience of systems such as smart grids, transportation networks, and industrial automation.

The overarching insight here is that digital identity in control and systems engineering is not only about authentication, but also about securing complex, interconnected infrastructures. By embedding identity into blockchain-based frameworks, researchers seek to ensure cyber-physical systems can operate reliably under conditions of high interdependence, where trust, resilience, and security are critical for societal and industrial stability.

5.10. Cultural Studies

In cultural studies, research highlights how digital identity is negotiated through age, gender, cultural norms, and life transitions. Serrate-González et al. analyse the online identities of 2076 Spanish adolescents, identifying gendered patterns in digital self-presentation. Their study shows that girls tend to link online personas to self-esteem, often using personal photos and filters, while boys favour anonymity or nicknames, reflecting broader pressures towards authenticity and idealisation for girls, and anonymity and gaming cultures for boys [65]. Cardon frames digital identity as a relational strategy, arguing that online self-presentation functions less as the revelation of objective facts and more as signalling and role-playing. Through concepts such as selective exposure and "publicly private" communication, he demonstrates how identity becomes a social performance shaped by surveillance, platform affordances, and cultural norms [66].

Extending this focus to life-course transitions, Orzech et al. examine how digital photography supports identity construction across generational stages. They find that

school-leavers use selfies and co-created images for self-presentation, while retirees emphasise place, family, and memory, showing how identity practices evolve with age to balance visibility, privacy, and social norms [67].

These studies demonstrate that digital identity in cultural studies is best understood as a socially embedded performance shaped by intersecting factors of gender, age, and cultural context. Whether expressed through adolescent self-esteem, relational role-play, or photographic practices across the life course, the overarching narrative is that digital identity reflects the dynamic interplay between personal agency and the cultural scripts that govern visibility, authenticity, and belonging in digital spaces.

5.11. Development

In this area, digital identity is examined through its implications for human development, social inclusion, and humanitarian aid. Masiero and Bailur analyse large-scale schemes such as Aadhaar, showing how they promise efficiency in service delivery but also generate risks of exclusion and surveillance [68]. They argue that while digital identity has the potential to expand access and empower minority and vulnerable groups, it can equally reproduce inequalities if implemented without sufficient safeguards. To address this tension, they call for a data justice lens that emphasises equity, transparency, and accountability, ensuring digital ID systems support empowerment rather than marginalisation.

The overarching narrative is that in development contexts, digital identity cannot be understood solely as a technical tool for efficiency. Instead, it must be located within broader debates about justice, rights, and inclusion, with particular attention given to the ways vulnerable groups experience empowerment and harm through identity infrastructures.

5.12. Education

In the education subdomain, digital identity is examined as a crucial factor shaping both teaching practices and student learning outcomes. Engeness shows how teachers construct digital identity not only through the use of digital learning environments, but also by actively designing them. Drawing on Galperin's pedagogical theory, she outlines design principles that strengthen professional digital competence and position teachers as active knowledge agents, thereby fostering professionalism and enhancing students' ability to "learn how to learn" in contemporary classrooms [69]. Goode explores how technology identity, formed through family, schooling, and access, influences college students' confidence and success in digital contexts. Goode argues that universities exacerbate inequities by assuming digital proficiency and calls for institutional interventions to support underprepared learners [70].

Heidari et al. extend this analysis to graduate education, showing that professional identity formation is shaped less by direct social network participation than by the online social capital these networks generate. They emphasise the importance of bridging and bonding ties within digital communities for professional identity development [71]. Poole advances the concept of Digital Funds of Identity, extending Funds of Knowledge theory into digital contexts through avatars, virtual learning environments, and hypertext. His work shows how teachers can draw on students' digital identities to promote empathy, inclusion, and critical pedagogy [72]. Adding a measurement perspective, Zimmer, McTigue, and Matsuda designed and validated the Digital Learning Identity Survey (DLIS), a tool tested with pre-service teachers that identifies six reliable factors of competence-based digital learning identity. Their findings show that acknowledging and assessing teachers' digital identities supports professional development and more effective integration of technology in classrooms [73].

Combined, these studies highlight how digital identity in education functions as both a professional construct and a developmental driver. It shapes teachers' competence and professional growth, influences students' confidence and equity of access, and provides conceptual and methodological tools for fostering inclusion and critical pedagogy.

5.13. Electrical and Electronic Engineering

In the electrical and electronic engineering subdomain, digital identity research highlights the technical design of secure authentication systems. Zhao et al. propose a blockchain-based two-factor identity authentication model for digital education, combining passwords and biometrics with encrypted, decentralised storage [74]. Their system demonstrates how distributed ledgers and cryptography can enhance the security, integrity, and reliability of large-scale identity management infrastructures.

At a thematic level, electrical and electronic engineering contributes to digital identity research by developing the cryptographic and infrastructural foundations upon which secure, scalable authentication systems are built.

5.14. Engineering

In engineering, digital identity research addresses the socio-technical assumptions underpinning system design. Bazarhanova and Smolander review digital identity architectures and identify three recurring non-technical dependencies: reliance on legacy infrastructure, trusted third parties, and user responsibility for managing cryptographic keys [75]. They argue that scalability and reliability in digital identity systems depend on how these assumptions are balanced and made explicit in engineering practice. Their analysis emphasises that technical robustness alone cannot guarantee sustainability unless the underlying social and organisational factors are acknowledged—and they note the fact that engineering perspectives on digital identity highlight the importance of recognising hidden assumptions in system architectures.

5.15. Geography, Planning and Development

In the geography, planning, and development subdomain, digital identity is framed as a spatial and political construct, closely tied to governance, inequality, and everyday practice. Cheesman examines self-sovereign identity (SSI) for refugees, arguing that its promise of autonomy is often undermined by geopolitical realities. Rather than empowering displaced populations, SSI may reinforce the power of states and corporations through humanitarian governance and border politics [76]. Manby critiques the Sustainable Development Goal of "legal identity for all," showing how biometric and digital ID rollouts in Africa can entrench exclusion and state control in contexts where citizenship is contested. Manby highlights how identity systems often reproduce spatial inequalities and warns that without safeguards, they risk deepening marginalisation [77].

Asamoah et al. propose Zero-Chain, a blockchain-based framework that assigns secure digital identities to residents, devices, and assets using group signatures and homomorphic encryption [78]. Their work illustrates how embedding digital identity in smart city infrastructures links individuals to urban services, positioning identity as a tool of spatial governance. Adjei et al. analyse social media practices in Ghana, revealing how users misjudge risks, misuse privacy settings, or rely on pseudonyms. They show how Africa's rapid mobile adoption, coupled with uneven digital literacy, shapes disclosure practices and underscores place-based inequalities in digital identity management [79].

Collectively, these studies demonstrate that geography and development perspectives on digital identity emphasise its embeddedness in power relations, spatial contexts, and infrastructural configuration.

5.16. Health and Informatics

In the health subdomain, digital identity is explored as both a means of personal expression and a critical infrastructure for secure healthcare delivery. Crowe and Watts examine identity play in massively multiplayer online role-playing games (MMORPGs), showing how young people use "gender-bending" avatars to negotiate agency, belonging, and resistance within cultural norms. They argue that such digital identity practices can enhance wellbeing by offering youth a space for self-understanding and exploration [80]. Udwan et al. extend this perspective to migration contexts, analysing how Syrian refugees in the Netherlands use social media for health, support, and identity. Their findings reveal that digital resilience practices—such as managing emotions, accessing health advice, and building supportive networks—are essential for wellbeing and integration under conditions of displacement [81].

Complementing these socially oriented studies, Javed et al. propose Health-ID, a blockchain-based system that provides patients and providers with unique, regulator-attested health IDs. Their system demonstrates how decentralised infrastructures can secure patient data, improve interoperability, and support compliance in telehealth environments [82]. Similarly, Coats and Acharya present a cloud-based framework that enables patients to access electronic health records (EHRs) with familiar federated credentials (e.g., Google). By reducing the need for provider-specific logins, their approach enhances usability, interoperability, and regulatory compliance in healthcare access [83]. Rohner focuses on identity management within hospitals, developing a maturity model that integrates responsibility, organisation, and IT functions. His work shows how coordinated identity management ensures timely, secure access to patient data for health professionals, thereby improving safety, compliance, and efficiency [84].

Taken together, these studies demonstrate that digital identity in health operates across two key dimensions. On the one hand, identity practices in games and social media provide spaces for self-expression, resilience, and emotional wellbeing. On the other, technical infrastructures such as blockchain systems, federated credentials, and hospital maturity models secure patient data, enhance interoperability, and ensure safe clinical practice. The overarching narrative is that digital identity in health spans personal, social, and institutional layers, shaping both individual wellbeing and the structural integrity of healthcare systems.

5.17. Human-Computer Interaction

In the human–computer interaction (HCI) subdomain, digital identity is analysed as a critical mediator between security, culture, and emerging virtual environments. Kaushik and Ghandi propose a hierarchical identity-based cryptography scheme for securing cloud data, showing how trusted identity mechanisms are central to ensuring reliable and secure user interaction in distributed systems [85]. Niezen takes a cultural perspective, examining how indigenous peoples use the Internet to construct digital identities that blend local traditions with global technological and legal frameworks. He argues that digital identity functions simultaneously as cultural expression and political strategy, co-created through community practices, ICTs, and global audiences [86].

Recent work has extended these insights into virtual environments. Mitrushchenkova argues that the metaverse generates multidimensional identities that blur distinctions between real and virtual selves. While such environments create opportunities for immersion and empowerment, they also heighten risks of surveillance, manipulation, and rights violations. Mitrushchenkova stresses that identity design in HCI must balance immersion, usability, and human rights to ensure safe and empowering digital spaces [87]. Ruiu et al. build on this by exploring Human Digital Twins (HDTs) in the metaverse—avatars that

integrate biometric and behavioural data to produce embodied and persistent digital identities. They highlight both the potential for rich identity representation and the dangers of identity theft and surveillance, advocating self-sovereign identity and advanced biometrics to balance usability, security, and user control [88]. Finally, Soldatova et al. show how adolescents construct richer, more integrated digital identities than parents, who tend to present narrower, socially dominated online selves. Their findings suggest that younger generations are better able to reconcile online and offline identities, supporting adaptability in mixed-reality environments [89].

Together, these studies show that digital identity in HCI is simultaneously technical, cultural, and experiential. It encompasses cryptographic infrastructures that underpin secure interaction, cultural practices that shape identity expression, and immersive environments that reconfigure selfhood through avatars and digital twins.

5.18. Industrial Relations

In the industrial relations subdomain, digital identity is examined through the lens of labour, governance, and power. Mir et al. analyse AI-enabled digital identity systems (AIeDIS), which promise greater accuracy, reduced fraud, and lower user burden while introducing new challenges of transparency and regulation. They argue that AIeDIS transforms stakeholder roles by reshaping how trust, accountability, and power are distributed among states, organisations, and workers [90]. In this context, digital identity becomes central not only to compliance and regulation, but also to questions of worker rights, participation, and fairness in the digital economy.

5.19. Information Systems and Management

In the information systems and management subdomain, research on digital identity is dominated by assessments of blockchain and SSI systems, alongside explorations of identity in emerging infrastructures such as the Internet of Things (IoT). Dunphy and Petitcolas evaluate blockchain-based identity schemes including uPort, ShoCard, and Sovrin using Cameron's "laws of identity". They find that while distributed ledger technologies (DLT) promise decentralisation, transparency, and user control, they remain dependent on intermediaries, suffer usability issues, and pose regulatory challenges [91]. Rouhani and Deters focus on smart contracts, surveying their security flaws, tools, and performance limits. They argue that smart contracts can support decentralised identity and SSI by reducing reliance on third parties and improving interoperability, though they highlight ongoing governance and integration obstacles [92].

Liu et al. review blockchain-based identity management systems, again comparing initiatives such as Sovrin, uPort, and ShoCard against Cameron's framework. Their study reinforces that blockchain enhances decentralisation and self-sovereign control, but unresolved issues of scalability, governance, and key management hinder adoption [93]. Sarma and Girao address the IoT context, arguing that the proliferation of devices multiplies identity challenges and raises risks of surveillance and control. They propose the Identinet, in which identity anchors all communication, and the digital shadow, a persistent identity layer that maintains consistency across contexts [94]. Sullivan and Burger examine Estonia's e-Residency programme, illustrating how blockchain-based identity can extend from national to transnational applications. While the scheme highlights opportunities for decentralised services and individual empowerment, it also faces risks of weak vetting, false identities, and financial crime, pointing to the need for strong legal and regulatory safeguards [95]. Finally, Satybaldy, Nowostawski, and Ellingsen propose an evaluation framework for SSI systems, applying it to Sovrin, uPort, ShoCard, Civic, and Blockstack. They find that while SSI enhances user control and transparency, it remains challenged

by centralisation risks, usability and recovery issues, and economic barriers, concluding that sustainable adoption requires stronger governance and non-profit or academic leadership [96].

These studies show that information systems and management research views digital identity as both a technical and institutional infrastructure. Blockchain and SSI are consistently identified as promising models for decentralisation and user empowerment, yet they remain limited by governance, usability, and integration challenges. Meanwhile, studies of IoT and national-to-transnational programmes illustrate the expanding contexts in which digital identity operates. The overarching narrative is that digital identity in information systems and management represents a field in transition—technically innovative but institutionally immature, requiring governance frameworks, usability solutions, and sustainable models of stewardship to realise its full potential.

5.20. Language and Linguistics

In the field of language and linguistics, digital identity is examined as a phenomenon constructed through discourse practices. Xu and Jing analyse ambient identity in anonymous danmu comments, showing how shared perspectives and converging attitudes foster the emergence of collective digital selves. Their study demonstrates that evaluative language and humour markers function as key resources for building communal identities within anonymous online interactions [97]. This research shows that language and discourse are central to digital identity, especially where anonymity hides individual markers. Linguistic cues and pragmatic strategies foster communal belonging, revealing that identity online arises not just from technology or personal agency, but also from shared communicative practices.

5.21. Law

In law, digital identity is examined as both a technical and legal construct, shaped by regulatory frameworks, rights protections, and governance standards. Dieye et al. propose a SSI system that uses blockchain and ZKPs to enable users to prove attributes without revealing personal data. Their design complies with GDPR and eIDAS, embedding privacy by design and providing legally verifiable proofs that uphold rights to data protection and identity autonomy [98]. Sharif et al. review eIDAS-regulated schemes in Europe, analysing authentication methods, standards, and mobile solutions while discussing the transition to eIDAS 2.0 and the European Digital Identity Wallet. Their findings show how regulation enforces interoperability, assurance, and privacy, while national-level implementations reveal trade-offs between compliance, usability, and innovation [99].

De Hert situates digital identity firmly within EU data protection law, calling for privacy-enhancing identity management grounded in principles of purpose limitation, transparency, security, and user rights. Furthermore, De Hert highlights German Constitutional Court rulings on informational self-determination and IT system confidentiality, framing these as steps towards recognising a fundamental right to digital identity protection [100]. Sperfeldt broadens the frame by analysing legal identity within the Sustainable Development Goals (SDG 16.9), emphasising how identity is entangled with governance, development, security, and market perspectives. Sperfeldt identifies three global trends—reliance on birth registration, expansion of digital ID, and risks of exclusion—warning that poorly governed systems may exacerbate inequality [101]. Finally, Ayed and Ghernaouti-Hélie assert the necessity of building privacy into digital identity management from the outset. Drawing on international, national, and sectoral laws, they identify requirements such as purpose limitation, consent, data minimisation, retention limits, and prohibitions on secondary use. Their analysis shows that lawful identity manage-

ment requires accountability, transparency, and enforceable safeguards against misuse, surveillance, and discrimination [102].

These studies demonstrate that law positions digital identity as a site where rights, regulation, and technology converge. While SSI and blockchain approaches highlight possibilities for embedding privacy by design, regulatory frameworks such as eIDAS underscore the challenges of balancing interoperability, compliance, and usability. Legal perspectives also emphasise the risks of exclusion and inequality when identity is poorly governed, stressing that digital identity must be treated not only as a technical system, but also as a legally protected right and a cornerstone of democratic participation.

5.22. Library and Information Sciences

In the library and information sciences field, digital identity is framed as central to knowledge visibility, access, and management. Fernández-Marcial and González-Solar study researchers at the University of A Coruña, finding uneven adoption of platforms such as ORCID and ResearchGate, though usage rates exceed global averages. They argue that digital identity is crucial for academic visibility and reputation, calling on libraries to provide training and integrate identity systems to better support researchers [103]. Robles-Carrillo conceptualises digital identity as a complex construct shaped by contextual, conceptual, and functional dilemmas. He presents it as a gateway to information access and management, emphasising the need to balance interoperability, privacy, and governance in increasingly interconnected digital ecosystems [104].

Library and information sciences research, therefore, positions digital identity as both an enabler of scholarly visibility and a systemic challenge of governance.

5.23. Management Information Systems

Sullivan traces the evolution of digital identity management from early authentication mechanisms to integrated systems that align with security, governance, and compliance. Sullivan demonstrates that identity is not only a technical function, but also a managerial and strategic asset. Within this framing, digital identity underpins secure access, regulatory compliance, and operational efficiency while simultaneously enabling innovation and enterprise integration [105].

5.24. Management of Technology and Innovation

In the management of technology and innovation subdomain, digital identity is positioned as a catalyst for transformation in governance and business. Al-Khouri examines identity systems in the Gulf Cooperation Council (GCC), which integrate smart IDs, biometrics, and public key infrastructures (PKI). His analysis shows how such systems reduce fraud, lower costs, and enable new e-government and e-business models. Digital identity is thus framed not merely as an administrative tool but as a driver of innovation and entrepreneurship, embedding trust to support modernisation and sustainable growth [106].

5.25. Marketing

In the marketing subdomain, digital identity is analysed as a signalling mechanism that shapes consumer behaviour and brand interaction. Rogova and Matta propose a model of digital identity signalling, showing that stronger identities drive more visible online behaviours and translate into offline decisions such as purchases or boycotts. Their findings highlight how consumers use digital platforms to signal identity, influencing how they engage with brands and communities. They suggest that marketers can leverage user-generated content and identity alignment to build stronger relationships, while also warning of the risks of reputational backlash when identity claims conflict with consumer expectations [107].

5.26. Media Technology

In media technology, digital identity is framed as a central element in the reshaping of culture through new media. Çoteli argues that digital platforms allow individuals to construct identities that diverge from their offline selves, and that these identities collectively contribute to the emergence of a global digital culture. Çoteli's analysis highlights the role of platforms and algorithms in shaping both identity construction and cultural expression, underscoring the deep interplay between technology and digital identity [108].

5.27. Political Science and International Relations

In the political science and international relations subdomain, digital identity is framed as a deeply political construct that redistributes power among states, markets, and citizens. Wang and De Filippi argue that centralised identity systems embed surveillance and political control, while self-sovereign blockchain-based models redistribute authority by allowing individuals—particularly migrants and refugees—to selectively disclose credentials. In doing so, they frame digital identity as a question of sovereignty and human rights [109]. Mir et al. analyse Aadhaar in India, showing how digital identity balances state priorities of welfare delivery, migration control, and surveillance against citizen concerns of privacy and inclusion. They argue that political legitimacy in such schemes depends heavily on design choices, particularly the prioritisation of uniqueness and security over scalability [110].

Extending this critique, Masiero and Arvidsson contend that Aadhaar generates degenerative political outcomes by excluding entitled citizens from welfare, misdirecting monitoring towards ration dealers while neglecting systemic leakages, and shifting social protection from food subsidies to cash transfers. They show how such transformations weaken welfare institutions and reshape state–citizen relations [111]. Shuaib et al. highlight how SSI can reconfigure political power in land governance by decentralising control, reducing corruption, and enabling verifiable property claims. They argue that SSI strengthens citizen sovereignty, builds trust in governance, and links digital identity to environmental sustainability [112]. Feulner et al. extend this line of analysis to cultural and economic participation, showing how SSI reshapes market governance in ticketing systems. By enabling stronger user–ticket binding, privacy-preserving verification, and control of secondary markets, they demonstrate how digital identity can shift authority away from scalpers and platforms towards state-recognised, verifiable credentials [113].

Taken together, these studies show that digital identity in political science and international relations is inseparable from questions of power, sovereignty, and legitimacy. Self-sovereign identity is framed as politically transformative, redistributing authority from states and corporations towards individuals, while state-centric programmes like Aadhaar illustrate how identity can entrench surveillance, exclusion, and institutional fragility. The overarching narrative is that digital identity is a political technology that simultaneously enables empowerment and control, with outcomes that depend on the governance choices and institutional contexts in which it is embedded.

5.28. Pollution

In environmental studies, digital identity is linked to patterns of consumption and their ecological consequences. Lou et al. argue that mobile identity, shaped by symbolism and design aesthetics, drives non-functional smartphone behaviours such as personalisation, public display, and protective use. They show this symbolic attachment to devices reinforces materialism and excessive consumption, indirectly intensifying environmental impacts [114].

5.29. Public Administration

In public administration, digital identity is examined as a transformative element in the governance of citizen–state relations. Lips argues that identity management reshapes these relations through tensions between three models: the Surveillance State, in which identity infrastructures enable monitoring and profiling; the Service State, where identity systems provide joined-up, citizen-focused services; and the Fair State, which reflects citizen expectations of transparency and equitable treatment. Drawing on studies in the UK and New Zealand, Lips shows how these perspectives often coexist, highlighting both empowerment and the erosion of trust as digital identity becomes central to governance [115]. Extending this analysis, Lips, Taylor, and Organ evaluate UK e-government deployments such as smart cards, online driver licensing, and automated number plate recognition (ANPR). They find that identity management simultaneously facilitates surveillance and service delivery, but also reconceptualises citizenship by shifting from universal rights towards conditional, data-driven access, raising significant implications for governance and democracy [116].

Sullivan and Tyson take a broader perspective, arguing that digital identity has evolved from a national administrative tool into an emerging international legal concept. They suggest that blockchain technologies offer both governments and individuals new mechanisms of verification and control, and that global digital identity is increasingly anchored in UN Sustainable Development Goal 16.9. They contend that international law must adapt to recognise digital identity as a human right and to regulate how states manage citizen identity information [117].

Together, these studies show that digital identity in public administration is both an enabler of efficient services and a mechanism of surveillance and control. The overarching narrative is that identity management systems redefine citizenship, shifting the balance between empowerment and conditional access, while simultaneously expanding from national infrastructures to global legal frameworks. This dual trajectory highlights digital identity as a central issue in governance, trust, and the evolving relationship between states and citizens.

5.30. Public Policy

In the public policy subdomain, digital identity is framed as a mechanism for managing trust, legitimacy, and coordination across state, market, and enterprise contexts. Seltsikas and O'Keefe analyse electronic identity management in government through a public value lens, arguing that outcomes such as fraud reduction, cost savings, and convenience depend less on technical efficiency than on the mitigation of relational risk between state and citizen. They contend that identity systems should be viewed not as absolute solutions but as tools for balancing security, efficiency, and legitimacy [118]. Zloteanu et al. extend this perspective to the sharing economy, showing that trust and reputation information (TRI) strongly shapes user judgments. Their experiments reveal that even minimal TRI (such as three rating elements) makes hosts appear more trustworthy, credible, and sociable, thereby increasing rental decisions. At the same time, they warn that platform identity policies risk promoting over-disclosure without delivering additional benefit [119].

L'Amrani et al. evaluate digital identity models—isolated, centralised, user-centric, and federated—against Cameron's "laws of identity." Their comparative study finds that federated identity most effectively balances minimal disclosure, justifiable parties, and pluralism, making it the strongest candidate for addressing cross-domain governance, trust, and policy coordination [120]. Kumar and Pradhan adopt a trust management perspective, contrasting social identities, which build trust through physical interaction and cultural continuity, with digital identities, which rely on authentication, past transactions,

and third-party validation. They argue that digital trust is inherently fragile, dynamic, and vulnerable to theft, necessitating robust systems for secure communication, reliable e-governance, and sustainable participation [121]. Jennings and Finkelstein focus on enterprise contexts, contending that digital identity is foundational to trust and reputation management. Without a unified identity resource across disparate systems, organisations cannot effectively assess reputation or accountability. They propose Digital Identity Pattern Extraction (DIPE) to integrate social software data, mitigate information overload, and enable reputation-based workflows aligned with organisational policy [122].

These studies demonstrate that digital identity in public policy is fundamentally about the management of trust across diverse governance contexts. Whether in government services, platform economies, cross-domain interoperability, or enterprise systems, digital identity is positioned as a policy tool that enables secure participation while simultaneously exposing new risks.

5.31. Safety, Risk, Reliability and Quality

In the safety, risk, reliability, and quality subdomain, digital identity is framed as a critical enabler of trust, resilience, and fraud prevention across both organisational and infrastructural contexts. Xu et al. argue that maritime cargo supply chains require binding the physical world of cargo movements to the cyber world of blockchain records through robust identity management. Their scheme issues vetted digital identities to firms, employees, and smart devices, organised hierarchically to ensure blockchain entries accurately reflect real-world custody. This approach reduces fraud, loss, and inspection burdens while improving resilience and trust in global logistics [123].

Ates, Ravet, and colleagues propose an Identity-Centric Internet architecture, where personal data is managed through "Identity in the Cloud Agents" (IC-Agents) under user control. By separating data storage from service provision and enforcing minimal disclosure, their model mitigates fragmentation, privacy breaches, and service-provider exploitation. They contend that such an approach embeds auditability, trust, and resilience into the very architecture of the Internet [124]. Wood takes an organisational perspective, arguing that safety and reliability hinge on robust identity management. He warns that identity theft—via phishing, weak passwords, social engineering, or device compromise—can render all other security defences ineffective. Wood emphasises that mitigation requires comprehensive policies, staff training, encryption, and secure authentication [125].

These studies demonstrate that digital identity in safety and reliability contexts operates as both a technical safeguard and an organisational strategy. Whether ensuring the integrity of global logistics chains, embedding resilience into Internet infrastructures, or protecting enterprises from theft and fraud, digital identity provides the foundation for trustworthy interaction. Identity management, therefore, is inseparable from risk management: it underpins reliability, mitigates vulnerabilities, and secures both physical and digital systems against failure and exploitation.

5.32. Security and Privacy

In the security and privacy area, digital identity is framed as both a technical safeguard and a source of risk in highly connected environments. Zhu and Badr argue that identity management in the Internet of Things (IoT) is inseparable from security and privacy. They critique centralised models that rely on trusted third parties, highlighting their vulnerability to single points of failure, phishing, and large-scale breaches. As an alternative, they propose blockchain-based SSI, which enables selective disclosure with zero-knowledge proofs (ZKPs) and user-controlled access—though challenges of scalability, interoperability, and privacy-preserving performance remain unresolved [126]. Yin et al. extend this focus

with SmartDID, a blockchain-based distributed identity framework designed for IoT. Using a dual-credential model, pseudonymous identifiers, and ZKPs, SmartDID balances Sybil-resistance, unlinkability, and supervisability, offering a tailored solution for IoT security and sustainability [127].

Sule, Zennaro, and Thomas examine national identity systems, arguing that cybersecurity resilience depends on embedding privacy and data protection into identity infrastructures. They note that without trust, citizens may reject schemes—as seen in the UK and India—and propose a Digital Identity Ecosystem governed by robust legal frameworks, user consent, and technical safeguards such as their Data Colouring technique, which combines PKI, biometrics, and watermarking to secure identity data across cloud and non-cloud platforms [128]. Stokkink et al. similarly critique SSI for its narrow focus on credential disclosure while overlooking network-level anonymity. In response, they developed TrustChain Identity (TCID) with the Dutch Government, integrating decentralised PKI, anonymisation overlays, pseudonym-based credentials, and auditing. Their system achieves passport-grade, privacy-preserving identity with practical latency, reinforcing the need to integrate anonymity into SSI design [129]. Finally, Beduschi highlights the human rights implications of digital identity systems. While such technologies can enhance access to services for undocumented or marginalised populations, reliance on biometric and blockchain infrastructures introduces risks of exclusion, surveillance misuse, and irreversible data harms. Beduschi argues that privacy- and non-discrimination-by-design safeguards aligned with GDPR and international human rights norms are essential to mitigate these risks [130].

These studies show that security and privacy in digital identity extend beyond cryptographic protections to encompass governance, trust, and human rights. Technical innovations such as blockchain, ZKPs, and anonymisation overlays promise stronger safeguards, yet unresolved challenges of scalability, usability, and inclusivity remain.

5.33. Social Media

In social media, digital identity is explored as a dynamic and performative construct, negotiated across personal, professional, and socio-technical contexts. Fisch and Block analyse 760 entrepreneurs' tweets before, during, and after business failure, showing how language reflects financial distress (greater focus on money and work), social loss (reduced references to friends and leisure), and psychological strain (lower emotional tone and authenticity). At the same time, they identify positive adaptations through increased reflection, self-assurance, and achievement drive, highlighting how entrepreneurs' digital identities evolve in response to offline crises [131]. Feher examines social media users in Central/Eastern Europe and Southeast Asia, finding that individuals consciously strategise their self-presentation, with around 70% of digital footprints actively managed and 30% shaped by digital dynamics beyond user control. While CEE users emphasise expressive engagement and dual offline–online identities, SEA users focus more on account management and reputation control. Both, however, face vulnerabilities such as identity theft, reputational harm, and surveillance [132].

Cho and Jimerson focus on school administrators' use of Twitter, identifying two carefully curated roles: instructional leaders who use hashtags and resource sharing to build professional learning networks, and institutional representatives who promote school values and events. They show that digital identity in this context is shaped by impression management, audience expectations, and surveillance concerns, with administrators deliberately avoiding personal disclosures and compartmentalising accounts [133]. Ruan et al. extend this focus to health professions, showing that social media cultivates professional identity as a parallel, fluid dimension of selfhood. Originating from educational and role-

based needs, these identities are sustained through community engagement but must be aligned with offline selves to avoid conflict, demonstrating how digital identity is now integral to professional responsibility and medical education [134]. Döring, Bhana, and Albury explore digital sexual identities on social media, emphasising their ambivalence as socio-technical phenomena. While platforms provide visibility, community, and activism for heterosexual, LGBTIQ+, asexual, kink, polyamorous, and sex worker communities, they also expose users to stigma, harassment, surveillance, and algorithmic discrimination. These dynamics shape how sexual identities are validated, contested, or erased in digital contexts [135].

These studies show that digital identity on social media is both empowering and precarious. It enables self-expression, community formation, and professional development, but is simultaneously constrained by surveillance, reputational risks, and structural inequalities. Social media, therefore, functions as a key arena where digital identities are performed, negotiated, and contested—reflecting the interplay between personal agency, audience expectations, and the socio-technical architectures of platforms.

5.34. Social Psychology

Rieger et al. assert that the European Digital Identity project, though promising for privacy, security, and efficiency, faces major social-psychological adoption challenges: rushed timelines risk undermining trust, coercing Big Tech may not ensure inclusivity for smaller firms, and digitally less-literate or non-European citizens (such as refugees) risk exclusion. They argue that social justice, usability, and user trust must be prioritised to prevent the system from becoming just another "login with X" button [136] (10 citations).

5.35. Social Sciences

In the social sciences, digital identity is analysed as a socio-technical construct that intersects with urban life, health, social media, and governance. Han and Hawken frame identity through the lens of smart cities and the data economy, where citizens' "informational footprints" are captured by platforms and infrastructures. They caution that technocratic approaches risk reducing cities to one-dimensional metrics and instead advocate for integrating cultural nuance, face-to-face relations, and local community identities so that smart cities function as innovation ecosystems balancing technology with inclusion and social value [137]. Bussone et al. emphasise the centrality of trust, identity, privacy, and security (TIPS) in designing digital identity for vulnerable groups. Their study of people living with HIV in the UK shows participants' willingness to share medical and lifestyle data, but strong resistance to disclosing personally identifying attributes. They argue that fine-grained consent, banking-level security, and community-led rules of interaction are necessary for platforms to sustain dignity, safety, and empowerment [138].

Code situates digital identity in social media as a negotiation of agency and selfhood. Drawing on Bandura's social cognitive theory and Mead's concept of the "generalised other," Code shows how platforms mediate identity expression, experimentation, and disclosure, enabling individual, proxy, and collective agency that shape well-being, belonging, and identity development in sociocultural contexts [139]. Sarav and Kerikmäe analyse Estonia's e-residency, a state-backed digital identity for non-nationals, showing how it reconfigures citizenship and economic participation beyond territorial boundaries. They argue that while it extends e-governance globally, it also raises concerns about inclusion, administrative capacity, and GDPR-aligned data protection as digital identity becomes a tool of membership and power [140].

Collectively, these studies show that social sciences scholarship foregrounds digital identity as a lens for understanding broader social dynamics: from data-driven governance

in smart cities, to privacy and empowerment in health, to agency and belonging in social media, and new forms of membership in state-sponsored digital programmes. Digital identity in the social sciences highlights the tension between technological innovation and social value, demonstrating how identity systems both enable participation and risk exclusion, shaping social life, governance, and community in significant ways.

5.36. Sociology and Political Science

In the sociology and political science subdomain, digital identity is analysed as a site of ambivalence situated between empowerment and control. Weitzberg et al. examine identity systems in humanitarian aid, showing how they simultaneously enable access, belonging, and efficiency while reproducing surveillance, exclusion, and sovereignty struggles. They critique the polarised debates that frame identity systems as either emancipatory or oppressive, demonstrating instead that recipients often experience biometrics and IDs ambivalently—as both opportunities for recognition and mechanisms of risk. They call for a depolarised social science agenda that attends to both "power over" and "power to" in digital identity interventions [141].

5.37. Software

In software research, digital identity is explored through challenges of authenticity, decentralisation, social practice, and negotiation. Allison, Currall, Moss, and Stuart highlight the instability of digital objects, arguing that because bitstreams are infinitely replicable, hardware and software environments constantly evolve, and "originals" lose fixity, authenticity and ownership cannot be guaranteed by technical measures alone. Instead, they contend that processes, cultural mechanisms, and contextual metadata are required to preserve salient features across transformations, thereby sustaining trust, credibility, and legal reliability [142]. Liu et al. review blockchain as a foundation for digital identity in software, emphasising its potential for decentralisation, immutability, anonymity, and resilience in authentication, access control, and data protection. While promising, they note unresolved challenges in scalability, interoperability, and regulation [143].

Emanuel and Stanton Fraser explore how mobile and networked technologies fuse teenagers' physical and digital identities. Through participatory design workshops, they show that teens value consistent personas across online and offline contexts for recognition, but express concerns about reduced control, especially around linking physical attributes such as location or biometrics to digital profiles. Their findings underscore the need for identity systems that balance technical functionality with privacy and social acceptability [144]. Squicciarini et al. focus on long-running digital interactions, extending the Trust-X framework to allow negotiation protocols that span multiple sessions. By introducing mechanisms for graceful suspension, credential similarity, and selective disclosure, they ensure correctness, validity, minimality, and non-disclosure while giving users greater control over when and how identity attributes are revealed [145]. Finally, Gulotta examines risks and motivations for sharing provocative images online, showing how curation practices and self-presentation strategies shape digital identity expression, while also introducing vulnerabilities to surveillance, reputational harm, and loss of control [146].

These studies demonstrate that digital identity in software is multifaceted: it requires technical robustness to preserve authenticity, decentralisation to ensure resilience, negotiation mechanisms to manage disclosure, and sensitivity to social practices that shape how identities are expressed and controlled. Software-based digital identity, therefore, is not solely a technical artefact but a socio-technical construct, requiring integration of cryptographic, procedural, and cultural mechanisms to sustain trust, privacy, and user autonomy across diverse contexts.

5.38. Theoretical Computer Science

In theoretical computer science, digital identity is studied as a socio-technical construct that requires formal models, cryptographic guarantees, and protocol design to balance privacy, security, and interoperability. Yang and Li present BZDIMS, a blockchain-based identity scheme that combines ZKPs with smart contracts to enable unlinkable, privacy-preserving verification. Their work demonstrates how distributed ledgers can address core issues of trust, decentralisation, and confidentiality in identity management [147]. Laurent et al. provide a multidisciplinary overview, defining digital identity as a composite of attributes, identifiers, and online traces shaped by both technical and social factors. Reviewing models ranging from siloed and centralised to federated and user-centric, they highlight key concepts such as anonymity and trust, while also identifying risks including identity theft and Sybil attacks. They argue that digital identity must be understood as a socio-technical construct, requiring formal approaches that integrate governance with privacy and usability concerns [148].

Gruner et al. analyse decentralised identity management (DIM), showing how blockchain eliminates the need for a central provider by making credential management and authentication publicly verifiable. While attribute aggregation reduces reliance on single entities, they conclude that decentralisation redistributes rather than eliminates trust, underscoring the need for rigorous trust models to guide secure and interoperable systems [149]. Kim et al. propose a blockchain-based federated identity system for the Industrial Internet of Things (IIoT), designed to overcome the weaknesses of OAuth and OpenID Connect. By ensuring neutrality, privacy, and scalability through decentralised trust models, they highlight the potential of blockchain identity for secure cross-domain interoperability [150]. Buccafurri et al. turn to Italy's SPID system, identifying risks of information leakage when service providers infer users' identity providers. They propose a protocol using random identifiers and multi-provider routing to anonymise authentication, showing how protocol-level innovations can mitigate privacy risks and reinforce trust in federated systems [151].

Theoretical computer science research frames digital identity as a problem of formalisation and protocol design, where decentralisation, anonymity, and trust must be modelled and guaranteed. Digital identity in this domain is not only a technical challenge of cryptography and distributed systems, but also a socio-technical problem requiring models that integrate governance, usability, and security to ensure trustworthy and interoperable infrastructures.

5.39. Urology

In urology, digital identity is framed as a professional and communicative asset. Gill, Zampini, and Mehta encourage urologists to proactively develop their digital presence through institutional profiles, professional networks such as LinkedIn and Doximity, and platforms including PubMed, Twitter, and YouTube. They argue that curated online identities enhance patient trust, signal professionalism, and foster collaboration, while also mitigating risks of misinformation and unmanaged third-party content [152].

In medical specialisations such as urology, this research and related studies show digital identity is integral to reputation, patient relationships, and professional engagement. By managing online presence strategically, clinicians can align their professional expertise with public visibility, ensuring both credibility and trust in an increasingly digital healthcare environment.

6. Temporal Dynamics

In this section, we show how the landscape has shifted over time, highlighting periods of acceleration or slowdown and notable inflection points. Readers can see which areas gain prominence and which recede as the field evolves.

6.1. Published Articles over Time

Figure 6 shows a long-run increase in annual output with three discernible phases: modest activity through the late 2000s and early 2010s, a step-up in the mid-2010s, and a pronounced acceleration from the late 2010s onward. Growth is especially steep in the most recent years, indicating sustained expansion rather than a plateau. The pattern suggests maturation of the field followed by rapid scaling, consistent with rising attention and investment in digital-identity research.

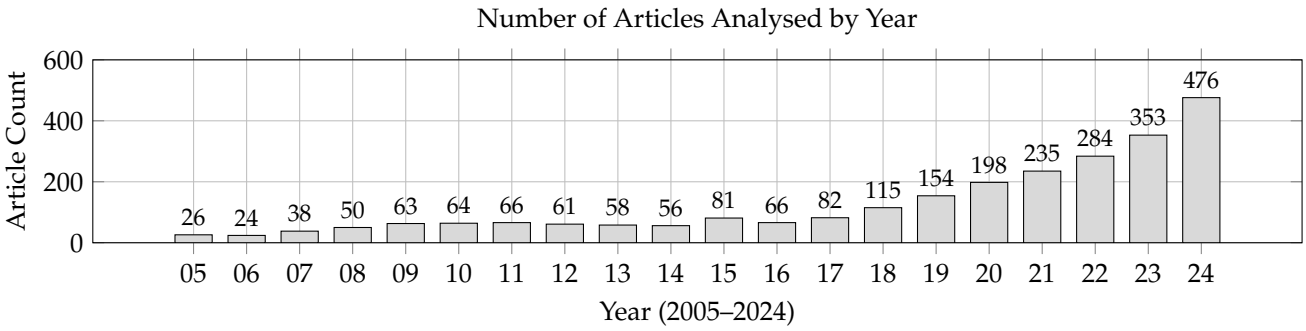

Figure 6. Total number of articles analysed per year from 2005 to 2024.

Computation

Annual publication counts in Figure 6 are computed by grouping the selected corpus records by Scopus publication year after applying the corpus selection procedure in Section 3. Each indexed record contributes one count to its publication year.

6.2. Keyword Trends over Time

Term matching is performed after the preprocessing and harmonisation steps described in Section 3.2, so that the plotted values reflect comparable term detection across years.

Figure 7 shows the share of articles containing terms associated with selected keywords from 2005 to 2024 and reveals three salient dynamics. First, digital identity remains the dominant term, peaking around 2010, dipping through the mid-2010s, and stabilising at a lower—yet still leading—level in the early 2020s. This reduction is consistent with field maturation, as the vocabulary diversifies and the relative weight of more specific terms increases. Second, a late-emerging decentralisation wave is evident: blockchain, decentralised, and self-sovereign identity are largely absent before 2016–2018, then rise sharply, with blockchain-related terms continuing to increase through 2024. Because the retrieval query is fixed over time (anchored on the phrase "digital identity"), this rise is not induced by time-varying query terms. However, term proportions can still be influenced by corpus composition (e.g., shifting discipline mix), editorial style, and indexing lag in the most recent years. For this reason, the trend plot includes comparator terms (*security*, *privacy*, *identity management*) to contextualise the decentralisation/ledger wave, and we use the separate 2023–2025 stratum to surface contemporary emphases without relying solely on long-run vocabulary totals. Third, management, security, and privacy vocabulary remains present but is comparatively flatter: identity management declines gradually, while security and privacy fluctuate without sustained upward trends. General tokens (digital, identity) maintain steady, mid-range prevalence. Collectively, these patterns indicate a shift

from traditional identity-management framing towards decentralised and SSI-oriented discourse, alongside a broadening terminology consistent with a maturing field.

6.2.1. Computation

For each term t and year y, the prevalence series in Figure 7 is computed as:

$$\text{prev}(t, y) = \frac{\#\{\text{articles in year } y \text{ whose processed abstract/keywords contain } t\}}{\#\{\text{articles in year } y\}} \quad (1)$$

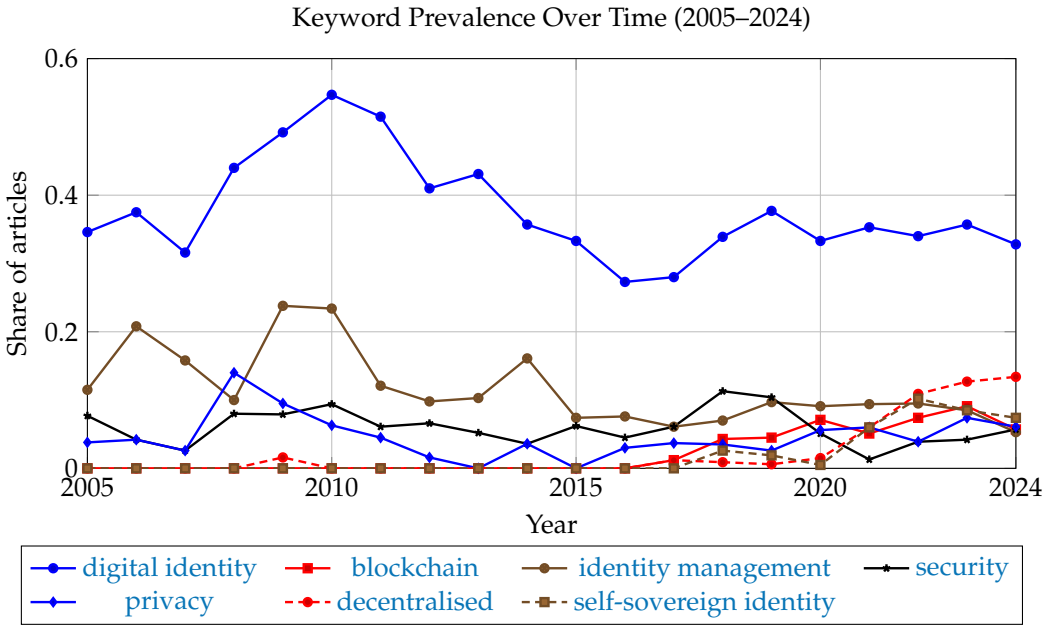

Figure 7. Keyword prevalence (share of articles) by year, selected terms. For Spearman trend tests for the plotted series see Table 8.

Table 8. Spearman trend tests for selected keyword-prevalence series (Figure 7). Spearman's ρ_s measures monotonic association between publication year (2005–2024; $n = 20$) and annual keyword prevalence. Reported p-values are two-sided.

Term	ρ_s	p-Value	Direction
digital identity	−0.397	0.083	decreasing
blockchain	0.872	5.31×10^{-7}	increasing
security	−0.226	0.337	decreasing
privacy	0.057	0.811	increasing
decentralised	0.775	5.93×10^{-5}	increasing
identity management	−0.750	1.38×10^{-4}	decreasing
self-sovereign identity	0.838	3.96×10^{-6}	increasing

6.2.2. Trend Testing

To complement the descriptive interpretation of Figure 7, we test whether each plotted prevalence series exhibits a statistically detectable monotonic trend over time. For each term, annual prevalence is defined as the share of articles in a given year that contain the term (i.e., the plotted proportion). We then compute Spearman's rank correlation between publication year (2005–2024; $n = 20$) and annual prevalence. These tests provide descriptive evidence of monotonic association (not causal inference) and are interpreted cautiously for end-of-window years that may be affected by indexing lag or partial-year coverage.

The Spearman trend tests reported in Table 8 provide statistical support for the directional patterns suggested by Figure 7. *Blockchain* shows a statistically detectable increasing

monotonic trend across the period, as do *decentralised* and *self-sovereign identity*, consistent with the rise of decentralisation-oriented discourse in the literature. In contrast, *identity management* exhibits a statistically detectable decreasing monotonic trend, indicating reduced relative prevalence of this legacy framing in the plotted series. For *digital identity*, the association with time is negative but does not reach conventional significance, suggesting relative stability with modest directional drift rather than a strong monotonic change. The remaining foundational terms, *security* and *privacy*, do not show statistically detectable monotonic trends over the full window, indicating that they remain persistent themes without a clear directional trajectory in this series. These tests are interpreted as descriptive evidence of monotonic association (not causal inference) and are considered alongside the end-of-window caution regarding indexing lag and partial-year coverage.

7. Authorship Patterns

In this section, we highlight the most active contributors and how their work concentrates—or diversifies—across topics. The focus is on visible profiles of output and subject focus, and where author activity overlaps.

Authors by Subject Area

Table 4 ranks the top 20 authors by article count and, for each, displays their four most frequent subject areas as colour-coded badges. Reading left to right: the first column lists authors, the second gives total articles, and the third shows the subject badges (colours are consistent across the paper, so the same subject uses the same colour everywhere). Subject badges reflect Scopus' multi-label assignments; they indicate frequent indexing categories rather than exclusive author specialisation.

Two patterns are apparent. First, the subject mix is technically skewed: Computer Networks and Communications, Computer Science (and Applications), Information Systems, and Artificial Intelligence recur across many authors, indicating a core computational centre of gravity. Second, several authors show cross-domain breadth, with badges spanning managerial, legal, or social strands (e.g., Information Systems and Management, Business/Management, Law, Education/HCI), suggesting socio-technical engagement beyond purely technical topics. Authors with four similar badges appear more specialised; those with diverse badges are comparatively broader. Overall, the panel provides a compact view of who contributes most and where they concentrate, while the consistent colour scheme enables quick cross-reference to subject patterns reported elsewhere in the results.

8. Thematic Analysis

Building on the corpus composition, temporal dynamics, and authorship patterns established earlier, this section maps the thematic structure of the literature. The clusters reported in this section are computed over *term embeddings* and should be read as concept/keyword groupings; documents are discussed as exemplars based on their association with salient cluster terms. We first summarise corpus-wide clusters derived from the baseline corpus (2005–2024; n = 2551), and then turn to a recent stratum (2023–2025; n = 1241) to highlight contemporary emphases.

8.1. Overview of Corpus-Wide Clusters (2005–2024)

Building on the corpus composition, temporal dynamics, and authorship patterns established earlier, this section maps the thematic structure of the literature and makes explicit how these computational patterns inform the paper's conceptual synthesis. We first summarise corpus-wide clusters derived from the full 2005–2024 dataset and then analyse a recent stratum (2023–2025) to surface contemporary emphases. Table 1 summarises the

corpus-wide (2005–2024) term clusters and representative keywords used to characterise each theme.

The resulting cluster structures serve a dual role: they provide an empirical thematic map of the field and supply the recurring concepts and associations that are subsequently consolidated into the preliminary ontological subgraphs (Figures 1–5).

1. Applications and Emerging Technologies—Practice-facing work applying digital identity across sectors (education, health, industry) with attention to usability, safety, and blockchain-adjacent innovation.
2. Architectures and Trust Frameworks—Core technical and architectural motifs (authentication, federation, wallets, credentials, revocation, (de)centralisation) that structure platforms and trust services.
3. Privacy, Rights, and Risk Management—Legal and risk discourse around confidentiality, protection, user rights, and information governance.
4. Cyber Environments and Emerging Ecosystems—System-level and socio-technical settings (cloud, networks, AI, metaverse/virtual worlds) in which identity is enacted.
5. Biometric Technologies—Modalities and systems for biometric access/verification (fingerprint, sensors, system integration).
6. Identity Management, Access Control, and Trust Services—Operational controls (authorisation, secure services, online/offline modes, privacy-preserving functions) bridging architecture and deployment.
7. Societal and Cultural Dimensions—Studies of platforms and practices (social media, education, literacy, gender) highlighting adoption, behaviour, and cultural factors.
8. Governance, Policy, Standards, and Regulations—Institutional and geopolitical layers (eIDAS, Aadhaar, public policy, inclusion, standards, national/regional programmes) shaping ecosystem evolution.

Note: Minor lexical variants (e.g., centralised/decentralised) and proper-noun anchors (e.g., eIDAS, Aadhaar) act as cluster markers rather than exhaustive descriptors; detailed distributions appear in the preceding subject-area analysis.

Computation

Cluster tables (Tables 1 and 2) summarise term-level clustering computed over the corpus vocabulary. After preprocessing (Section 3.2), Word2Vec embeddings are trained and K-means is applied to the resulting term vectors (Sections 3.3 and 3.4). The keywords listed per cluster are representative/high-salience terms used to characterise each concept grouping for interpretability.

8.2. Thematic Structure of Recent Literature (2023–2025)

Focusing on the most recent tranche of publications, this subsection profiles the thematic structure of the 2023–2025 literature and contrasts it with the corpus-wide baseline. The aim is to surface emphases that are amplified in the near term—whether through consolidation of established topics or the emergence of newer lines of work—without restating material already covered in the subject analysis.

We report (i) the dominant clusters in 2023–2025 with their defining terms (see Table 2), (ii) points of continuity and divergence relative to 2005–2024 clusters (see Table 3), and (iii) concise exemplars where helpful. Table 9 provides a crosswalk from the recent clusters to candidate ontology constructs and the illustrative subgraphs. Interpretation is tempered by window effects (a shorter horizon and partial-year coverage for 2025), but the section highlights where attention has recently intensified and how topical balance is shifting.

Table 9. Crosswalk from recent clusters (2023–2025) to candidate ontology constructs and illustrative subgraphs.

Empirical Cluster (Table 2)	Ontological Signal (Candidate Constructs)	Illustrative Subgraph (s)
1. Credentials, Wallets, and Trust Services	*Entities:* credential, wallet, issuer/verifier, trust service, contract. *Processes:* issuance, presentation, verification, status/revocation, (un)linkability. *Context:* public/private trust arrangements and service delivery constraints.	Figure 1 (Credentials); Figure 4 (Blockchain)
2. Enterprise Adoption and Immersive/Global Contexts	*Entities:* organisation, platform, environment (enterprise/immersive), cross-border setting. *Processes:* adoption, deployment, management, transformation. *Context:* regulatory constraints; global/virtual interactions amplifying risk and trust requirements.	Figure 3 (System); Figure 5 (Society)
3. Methodologies, Models, and Assurance Workflows	*Entities:* model, method, workflow, evidence/traceability artefacts. *Processes:* verification, assurance, evaluation, usability testing, systematic comparison. *Context:* repeatability and auditability as requirements that mediate design choices.	Figure 3 (System); Figure 2 (Security)
4. Security, Privacy, and Data-Protection Foundations	*Entities:* threat/risk, security control, privacy mechanism, rights/compliance construct. *Processes:* protection, preservation, mitigation, monitoring. *Context:* internet/network settings; trust as an emergent property shaped by controls and governance.	Figure 2 (Security); Figure 5 (Society)
5. Decentralised Identity and Persona/Presentation	*Entities:* user, identity/persona, avatar, platform. *Processes:* self-presentation, interaction, authentication under decentralised/sovereign models. *Context:* platform-mediated environments; authenticity vs. security and control trade-offs.	Figure 3 (System); Figure 5 (Society)
6. Socio-Cultural and Educational Practices Online	*Entities:* community, user groups (students/teachers), platform/media space. *Processes:* representation, engagement, practice formation, literacy development. *Context:* cultural norms, gender, language, power dynamics shaping identity practices and perceived harms.	Figure 5 (Society); Figure 3 (System)
7. Governance, Policy, and European Frameworks	*Entities:* government, legal framework (eIDAS/GDPR), programme/ecosystem instruments. *Processes:* implementation, compliance, cross-border interoperability/mobility. *Context:* regulation as a constraint and enabler linking trust services to adoption and accountability.	Figure 5 (Society); Figure 1 (Credentials)
8. Sectoral Innovations and Public-Interest Applications	*Entities:* sectoral contexts (health/education/cities/energy), service providers, applied infrastructures. *Processes:* service delivery, data exchange/access enablement, safety and sustainability aims. *Context:* public-interest requirements (inclusion, accountability) shaping system design and governance fit.	Figure 3 (System); Figure 4 (Blockchain)

To aid interpretability, we provide two compact visual summaries of the thematic structure. Figure 8 summarises the three-strata organisation that emerges from the clustering results (technical rails; governance and institutions; use and practice) and highlights the dominant linkages between technologies, governance models, and deployment contexts. This three-strata framing is used throughout the remainder of Section 7 to reduce category leakage by separating technical mechanisms, governance/institutional arrangements, and use/practice contexts, while explicitly treating a small set of concepts (e.g., trust, privacy, accountability) as cross-cutting where they span strata. Additionally, Figure 9 visualises the mapping from corpus-wide clusters (2005–2024) to the recent stratum (2023–2025), complementing Table 3.

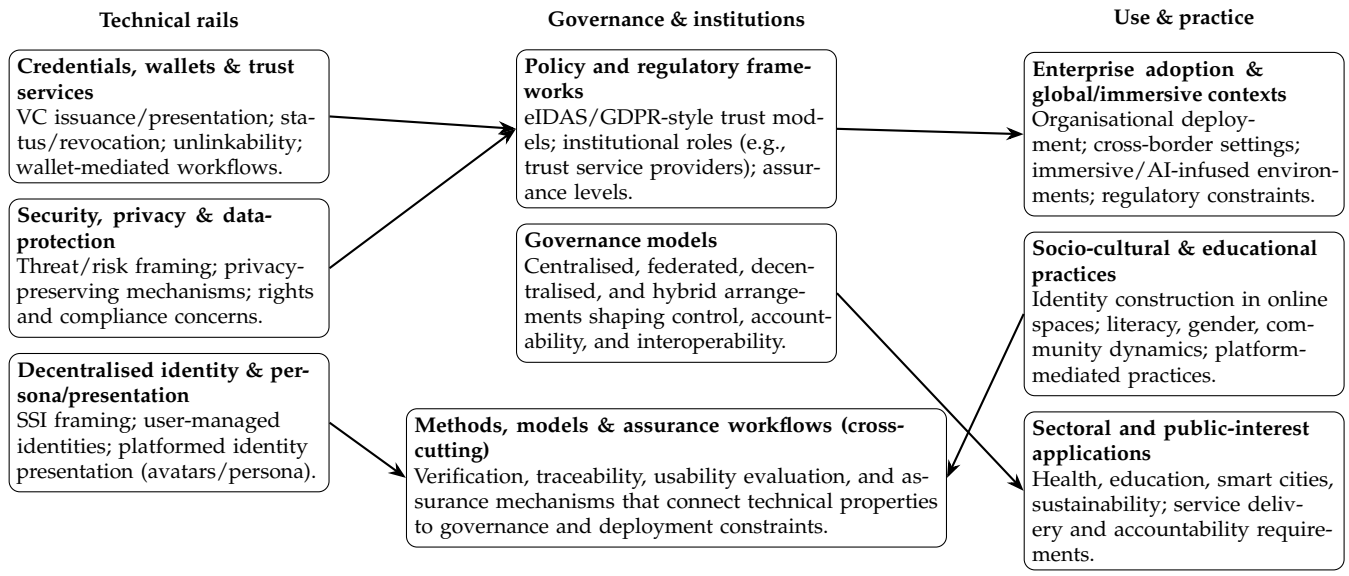

Figure 8. Schematic summary of thematic relationships observed in the clustering results, organised into three strata (technical rails; governance and institutions; use and practice) and highlighting key linkages between technologies, governance models, and deployment contexts.

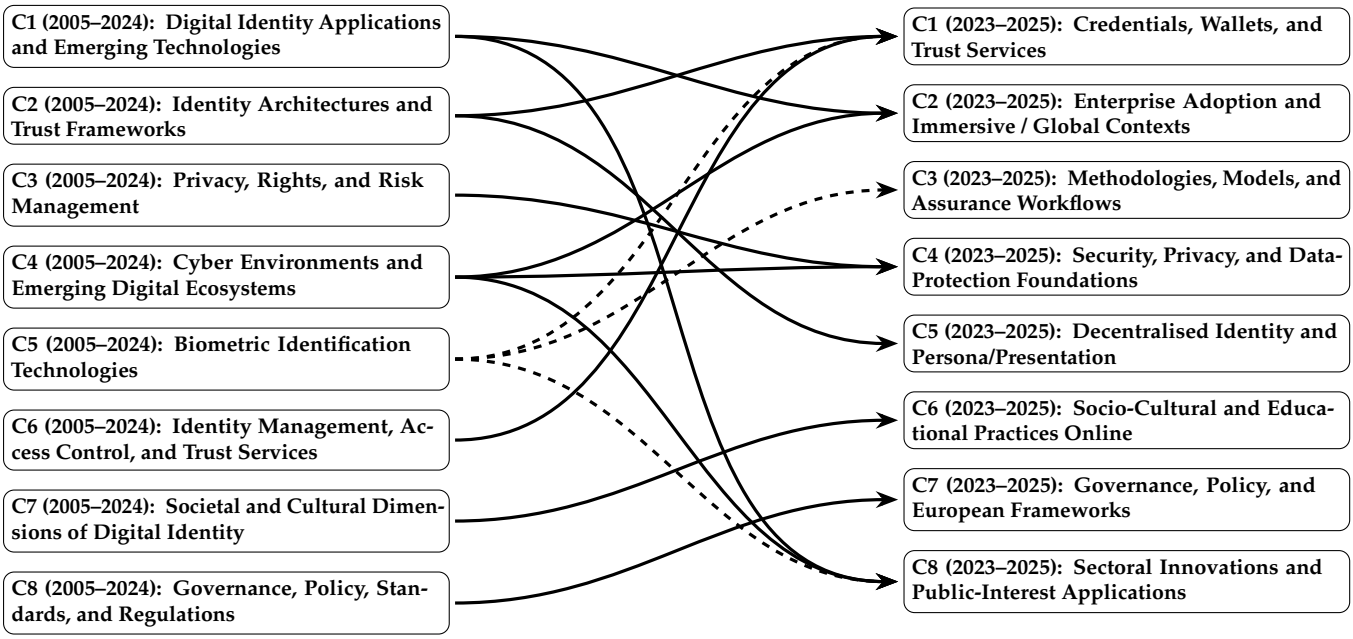

Figure 9. Visual summary of thematic evolution: mapping corpus-wide clusters (2005–2024; Table 1) to the recent cluster structure (2023–2025; Table 2), based on the cluster-set comparison (Table 3). Dashed links indicate redistribution of a formerly standalone theme across multiple contemporary clusters.

Computation

Ontology subgraphs (Figures 1–5) are presented as ontological fragments derived from the recent-stratum thematic structure. For each selected core term, we assemble a compact set of associated concepts from the recent cluster vocabulary (Table 2) and representative exemplars discussed in the corresponding subsection, and visualise these as a concept map to make the empirical "ontological signals" legible. Edges denote indicative associations for interpretation (not formally typed ontology relations), and the figures should be read as conceptual scaffolding rather than a machine-readable ontology artefact.

8.3. Credentials, Wallets, and Trust Services

Recent research on credentials, wallets, and trust services highlights the centrality of wallet-centric architectures for enabling secure, private, and interoperable digital identity. At the core of this work are mechanisms for access and authentication, issuance and revocation of verifiable credentials, selective disclosure, and recoverability—implemented under real-world deployment constraints.

Careja et al. propose a blockchain-anchored model where trusted authorities issue ECDSA-based proofs for user attributes, while personal data remains off-chain under user control. Ethereum smart contracts support verification, revocation, and unlinkability through wallet-centred workflows exposed via APIs for users, authorities, and verifiers. Their use cases in university access and anonymous decision support illustrate how separating data ownership from credential verification enables practical trust services for authentication [153]. Similarly, Nita and Mihailescu design a Web 3.0 authentication scheme built on SSI. In their model, users store credentials in wallets, selectively disclose attributes via ZKPs, and verifiers check integrity and revocation against a distributed ledger, thereby enhancing access control, privacy, and interoperability across services [154].

From a national infrastructure perspective, Mogensen and Aranha provide a user-centric security analysis of Denmark's passwordless MitID service. They identify vulnerabilities such as user-ID enumeration, denial-of-service attacks, and social engineering risks, arguing for additional safeguards such as request authentication, stronger identifier policies, and rate-limiting. While post-disclosure changes mitigated some phishing vectors, they show that targeted denial-of-service remained feasible, underscoring the risks in access and verification workflows [155].

Heiss et al. use zkSNARK-based verifiable off-chain computation (implemented with ZoKrates) to enable non-disclosing, on-chain verification of W3C-style verifiable credential conditions in Ethereum smart contracts, and they discuss replay resistance (via uniqueness proofs) and revocation/expiry extensions, demonstrating feasibility with non-trivial on-chain costs [156]. Lan and Jiang extend these approaches with a scheme combining Merkle trees, IPFS, and a weighted PBFT consensus (DPBFT). Their design introduces two-factor verification with non-interactive zero-knowledge proofs (NIZKs), ElGamal encryption, and Shamir secret sharing. Experiments report significantly reduced proof/gas costs and stronger composite security scores compared with CertChain and CertLedger, demonstrating efficiency gains for wallet-based trust services [157].

Studies belonging to this cluster illustrate how credentials and wallet-centric trust services form a rapidly evolving subdomain of digital identity. Whether through SSI-based selective disclosure, blockchain-enabled revocation transparency, or national authentication systems, the overarching narrative is that digital wallets are becoming the practical locus of trust. Yet this research also shows that such systems remain constrained by usability, cost, scalability, and vulnerability to targeted attacks, requiring ongoing innovation in cryptography, governance, and user experience to achieve resilient and inclusive adoption.

8.4. Enterprise Adoption and Immersive/Global Contexts

In the enterprise and global adoption subdomain, recent digital identity research focuses on business-led deployment, regulatory frameworks, and the challenges of extending identity infrastructures into immersive and cross-border contexts. Wu and Zhang review digital identity in the metaverse, arguing that avatar-based interactions intensify privacy risks and trust failures, necessitating a unified, government-backed authentication system. They highlight tensions between blockchain transparency and privacy, platform exploitation of data, and online harms, and propose a legal toolkit—including personal-data classification, consent rules, and personality-rights remedies—to secure access, authentica-

tion, and credential use across immersive environments [158]. Wang and Wang similarly examine metaverse identity through the lens of enterprise identity and access management (IAM). They trace the evolution from paper to "digital doubles," emphasising the need for role-based user characterisation, wallets and verifiable credentials, and privacy filters. At the same time, they recognise the continued role of centralised supervision under frameworks such as eIDAS to mitigate fraud and rights risks, offering a combined policy and design agenda for trustworthy metaverse adoption [159].

Beyond immersive environments, Quispe Sanabria et al. review blockchain for digital identity management, highlighting its potential to enhance security, privacy, user control, and efficiency through decentralised verification mechanisms such as selective disclosure and traceability. They note, however, that real-world adoption remains contingent on addressing governance constraints and contextual challenges [160]. Hilowle et al. turn to national identity systems, synthesising 90 studies to identify eight human-centric determinants of adoption: security, privacy, trust, perceived risk, usability, flexibility, cybersecurity awareness, and cultural/social influences. They propose a multi-level UTAUT+TFI framework to show how enterprise and public-sector uptake depends as much on these social and organisational factors as on technical infrastructure [161].

Together, these studies demonstrate that enterprise and global adoption of digital identity is shaped by the interplay of technical innovation, governance, and human factors. In the metaverse, digital identity is both a risk vector and a necessary foundation for trust, requiring new blends of decentralisation and regulation. In enterprise and national systems, adoption depends not only on technical security but also on user perceptions, cultural factors, and regulatory alignment. The implication is that digital identity in enterprise and global contexts is a strategic enabler of transformation, yet its success hinges on embedding governance, usability, and trust into both immersive and institutional frameworks.

8.5. Methodologies, Models, and Assurance Workflows

In the methodologies and assurance cluster, recent research focuses on systematic approaches to modelling, verification, and evaluation in digital identity. Hilowle et al. develop and validate a human-centric cybersecurity model that integrates the Technology–Function–Institution (TFI) framework with the Theory of Planned Behaviour (TPB). Based on a survey of 203 Australians, they find that security, privacy, usability, and flexibility positively predict the intention to use national digital identity systems, while perceived risk and cultural/social interference negatively affect adoption. Interestingly, trust and cybersecurity awareness were not significant predictors. Their model explains approximately 76% of variance and provides a foundation for assurance workflows and governance interventions aimed at improving uptake [162].

Paier et al. present an interface-based threat model and automated ProVerif workflow to formally analyse multi-factor authentication (MFA) schemes in eIDAS digital ID cards. Applying the method to Italy's CIE Level-2 authentication (SMS-OTP, QR-code, push), they systematically enumerate hundreds of attacker scenarios, exposing flaws such as credential escalation and display leakage. They propose lightweight fixes (L2SMS* and L2PSH* with session-code verification), which their formal analysis confirms as effective, demonstrating the value of model-driven verification in improving protocol security [163].

At a more conceptual level, Boldrin critiques existing verifiable credential (VC) and RDF-based frameworks for being overly entity-oriented, proposing instead an attribute-centric, set-theoretic language for digital identity. Boldrin formalises identity statements as propositional formulas over attributes, linked via "confirmation means" such as keys or biometrics. Verification proceeds by chaining vouched documents to attributes, while extensions introduce trust relations. This approach aims to sharpen modelling prac-

tices, improve verification precision, and strengthen assurance workflows across identity frameworks [164].

These contributions illustrate how methodologies and assurance models move digital identity research beyond one-off case studies towards repeatable, systematic processes. By integrating human-centric adoption models, formal threat verification, and attribute-level abstractions, this strand of literature provides the tools needed to evaluate and harden identity systems against both technical and social risks. Robust assurance, therefore, requires blending socio-technical modelling with formal verification and conceptual clarity, ensuring digital identity systems are functional, trustworthy and auditable.

8.6. Security, Privacy, and Data-Protection Foundations

A security–privacy core persists: preserving, protection, rights, trust, theft. Work here consolidates privacy-by-design and protection against credential or account compromise in networked/Internet settings. Typical outputs include threat models, privacy guarantees (e.g., minimisation, policy compliance), and controls that balance confidentiality with verifiability.

Computation

In the foundations of security, privacy, and data protection, digital identity research emphasises privacy-by-design, zero-trust models, and robust assurance mechanisms to protect against credential compromise, surveillance, and misuse. Díaz Rivera et al. propose a zero-trust, privacy-preserving MFA framework in which authentication is distributed across blockchain validators to avoid single points of failure. Users prove one-time-password (OTP) knowledge via zk-SNARKs and are issued non-transferable NFT tokens for session access, with on-chain verification and revocation controls. Their prototype demonstrates competitive latency while strengthening resistance to impersonation and OTP abuse [165].

Wang, Gai, and Zhang also adopt a zero-trust perspective, presenting a conceptual NOPI model that links network trust, organisational collaboration, user big data, IT capabilities, and blockchain security. Validated with survey data (n = 309), the model shows strong factor fit and leads to a governance proposal based on consortium structures, dynamic auditing, biometric verification, encrypted channels, and policy principles for trustworthy identity management across public and private actors [166]. Complementing these conceptual frameworks, Comb and Martin mined 6157 “digital identity” patents (1948–2023) using NLP methods to map security, privacy, and trust trends. They reveal accelerating patent activity, the dominance of user/data-centric approaches, the rise of blockchain/ledger/credential motifs, and a shift from card-based verification towards wallet-mediated transactions, producing validated clusters to guide governance and protection strategies [167].

Buccafurri, Lax, and Russo propose a fog-computing architecture for remote clinical services that integrates eIDAS-compliant digital identity with anonymous credentials. Their design enables fog servers to verify access and perform revocation checks without learning user identities, while repeated accesses remain unlinkable through a credential-switch protocol. A security analysis confirms resistance to stolen-device and replay attacks, demonstrating GDPR-aligned privacy preservation in e-health contexts [168]. Finally, Song et al. develop a blockchain-based identity system that separates verifiers from credential providers, using linkable ring signatures to anonymise verification. By combining commitments, non-interactive ZKPs, PS randomisable signatures, and dynamic accumulators, they achieve privacy, revocation, and on-chain auditability. Smart contracts provide transparent verification, with a car-rental prototype showing practical feasibility in terms of performance and gas costs [169].

These studies consolidate a core security–privacy agenda in digital identity research. They demonstrate how privacy-preserving cryptography, distributed authentication, fog architectures, and patent-driven innovation trends converge to embed resilience, auditability, and compliance into identity infrastructures.

8.7. Identity and Persona/Presentation

Recent research on identity and persona highlights the performative and user-centred aspects of digital identity across decentralised architectures, social platforms, and cultural institutions. Jena et al. review healthcare applications, showing how IoT and blockchain can strengthen confidentiality, integrity, and availability in patient identification, data exchange, and monitoring. They argue that decentralised, privacy-preserving identity solutions are critical to overcoming challenges of scalability and interoperability in clinical contexts [170].

Lareki et al. examine adolescents' creation of fake profiles and falsified ages on social media, finding that such practices—especially among older boys on platforms such as Facebook, Twitter, and Instagram—are strongly correlated with cyberbullying. Their study highlights how fabricated identities facilitate harmful online behaviours and underscores the importance of early digital literacy and stronger platform accountability [171].

Masiero critiques digital identity platforms more broadly, contending that their core–complements architecture inherently links identification, authentication, and authorisation with surveillance and exclusion. Drawing on cases from refugee aid (BIMS/Kakuma) and Eurodac, he argues that surveillance is not a contingent outcome but an intrinsic feature of platform-based identity systems, and calls for closer scrutiny of their socio-political effects [172]. Giannini and Bowen extend this discussion into cultural institutions, showing how museums are reshaped by digital identity through online heritage sharing, activism, and digitisation. They argue that museums now function as contested sites where cultural conflict, social justice, and heritage ownership are negotiated across physical and digital spaces [173].

Block et al. analyse founders' self-presentation on Twitter, operationalising Schumpeterian persona traits such as vision, optimism, and achievement. They find that future-oriented vision and optimism predict follow-on venture-capital funding, while strong achievement motives correlate negatively. Their study concludes that venture finance rewards particular persona presentations rather than a uniform "Schumpeterian identity," implying limits to alignment between entrepreneurial identity and capital markets, and highlighting a potential role for public funding in supporting technology transfer [174].

Together, these studies show that digital identity as persona and presentation extends across healthcare, social media, cultural heritage, and entrepreneurship. Whether expressed through decentralised credential frameworks, adolescent experimentation, institutional inclusivity, or entrepreneurial performance, digital identity is revealed as a user-centred construct negotiated through platforms and socio-technical systems.

8.8. Socio-Cultural and Educational Practices Online

In socio-cultural and educational areas, digital identity is examined as a lived practice negotiated in everyday online contexts, from celebrity performance and youth culture to teacher training and professional development. Martín Matas and Gil analyse Emma Watson's Instagram presence to show how celebrity identity is constructed through visual narrative. Using longitudinal mixed methods, they find that shifts towards brand-centred content (e.g., Prada and Renais Gin) coincide with altered engagement rates, demonstrating how changes in narrative form shape audience interaction [175]. Masitoh et al. focus on pre-service English-as-a-foreign-language (EFL) teachers in Indonesia, applying

Wenger's engagement–imagination–alignment framework. Their findings show that gamified teaching practices create both identity tensions and new "tech-savvy" teacher personas, underscoring the need for teacher education to explicitly foreground identity work and equitable access to technology [176].

Li et al. studied Chinese Spanish-language teachers during the COVID-19 lockdown, revealing how online teaching produced multiple professional identities—including curriculum innovator, vulnerable actor, and involuntary team-worker. Their analysis, based on interviews, discourse, lesson plans, and student feedback, shows how digital pedagogy is shaped by agency, experience, emotional strain, and institutional context. They argue that strengthening digital literacy and aligning evaluation and governance with online practices are essential to sustainable professional development [177]. Puspitasari et al. apply corpus-linguistic methods to WhatsApp messages from 100 Indonesian high-school students in the new capital (IKN). They identify three patterns—lexical choice, orthographic selection, and lexical bundles—through which students negotiate culture, affiliation, and self-presentation. Their findings demonstrate how youth construct digital identity through linguistic practices and suggest that inclusive, digitally literate language education is necessary for equitable participation in IKN [178].

These studies show that socio-cultural and educational practices online highlight digital identity as a dynamic process shaped by representation, literacy, institutional structures, and cultural norms.

8.9. Governance, Policy, and European Frameworks

Recent research in governance, policy and frameworks highlights how legal frameworks, public-sector choices, and ecosystem incentives shape the adoption of digital identity. Anchored by eIDAS, GDPR, and national or regional programmes, this literature emphasises implementation guidance, compliance, interoperability, and the institutional arrangements required for wallet deployment and trust services.

Degen and Teubner analyse Germany's consultation process for eIDAS 2.0, drawing on 80 stakeholder submissions and 14 expert interviews. They conceptualise how governments can orchestrate a public–private digital-identity ecosystem by mapping value flows, stakeholder tensions, and monetisation mechanisms. From this, they derive two orchestration models—Government ID-Infrastructure Wallet and Trust ID Wallet Federation—as frameworks for wallet provision, certification, and governance [179]. Schwalm focuses on the prospective impacts of eIDAS 2.0 on German and European identity systems, highlighting how the EU Digital Identity Wallet (EUDIW) integrates SSI principles within the eIDAS trust model. He details regulatory and technical shifts such as wallet obligations, assurance-level requirements, qualified trust service provider (QTSP) roles, and acceptance by public services and major platforms. His analysis identifies opportunities in data sovereignty and mutual recognition, alongside risks in usability, accessibility, surveillance, and standardisation gaps [180].

Martínez examines the inclusivity of eIDAS 2, focusing on how the EUDIW can address disability. He argues that beyond accessibility obligations (Articles 5bis, 15), the wallet should integrate disability-related support attributes, verified through qualified electronic attribute statements and authentic sources. Framed within Spanish civil-law reforms, his analysis outlines governance needs such as interoperability, training, and privacy-preserving verification to ensure disability rights are embedded into EUDIW implementation [181]. Expanding beyond Europe, Ibor et al. compare interoperability mechanisms in developing countries, contrasting X-Road and eIDAS. They identify gaps in legal, technical, and trust frameworks, and propose a process-based benchmarking approach—covering assurance levels and federation trust relationships—to guide reliable

cross-border identity and service delivery [182]. Inza offers a comprehensive overview of the eIDAS 2 reform and its definition of the EUDIW, detailing legal changes, governance structures, pilot use-cases, and supporting infrastructures such as EBSI and EUROPEUM-EDIC. He positions the EUDIW as the foundation for cross-border, privacy-respecting identification and qualified trust services across the EU [183].

These studies show that governance and policy debates situate digital identity at the intersection of regulation, trust, and interoperability. While eIDAS 2.0 is presented as an ambitious attempt to merge SSI-inspired features with state-backed guarantees, challenges remain in inclusivity, usability, and global interoperability.

8.10. Sectoral Innovations and Public-Interest Applications

In the sectoral innovations and public-interest areas, digital identity is positioned as a cross-cutting enabler for accountable, data-driven service delivery in domains such as healthcare, education, smart cities, and sustainability. Rafajac and Jakupović (eds.) advance an Integral Communication Framework that incorporates integral digital identity to personalise information exchange and feedback across sectors. Their framework seeks to improve collaboration, quality management, and citizen trust at scale. Supported by empirical user studies, it integrates governance safeguards including privacy control, multilingual tagging, and transparency. Sectoral applications range from e-government services and smart-city infrastructures to education/career matching and healthcare workflows, positioning digital identity as a public-interest infrastructure that links technical interoperability with sustainable, citizen-centred service delivery [184].

In sectoral and public-interest contexts, digital identity is less a standalone technology than a foundational layer for applied innovation. By embedding identity into multi-sector frameworks, research shows how trust, accountability, and usability can be institutionalised across critical services, enabling data exchange and access in ways that balance efficiency with inclusivity.

8.11. Cluster Set Comparison

The comparison shows strong through-lines alongside notable reorganisations. Privacy, security, and data-protection concerns persist with limited redefinition, while governance remains central but is framed more explicitly through European instruments (eIDAS, GDPR) and wallet programmes. Social and educational work continues, now with heightened attention to platformed practices and youth contexts.

By contrast with earlier work on broad "architectures and frameworks," the technical core has been restructured into two domains: (i) wallet-centric trust services (verifiable credentials, status/revocation, unlinkability), and (ii) a decentralised/persona layer that foregrounds multi-platform presentation (avatars, user-managed identities). Day-to-day identity management and access control are increasingly framed as operational facets of wallet/VC infrastructures rather than as a separate locus of research.

Applications broaden on two fronts: sectoral innovations (healthcare, education, cities/energy, sustainability) and enterprise/global adoption that includes immersive and AI-infused environments. What was previously a general "cyber ecosystems" vantage is redistributed into these concrete adoption contexts alongside a clearer security baseline. Biometrics does not disappear but is less often a standalone theme; its methods and risks surface within assurance workflows, wallet-based journeys, and domain deployments.

Overall, the 2023–2025 stratum retains the classic pillars (security/privacy, governance, socio-cultural analysis) while reorganising technical and applied work around *wallet-based trust services*, *decentralised/persona-centric models*, explicit *methods and assurance* contributions, and *context-specific* adoption pathways.

9. Limitations and Research Gaps

This section considers the limitations of the research, providing a basis for future work.

9.1. Coverage and Corpus Bias

Our evidence base is constrained by database and time-window choices. The baseline corpus (2005–2024, with a 2023–2025 stratum) is drawn from indexed scholarly sources; it under-represents grey literature, standards drafts, policy documents, and industry reports that shape practice. Indexing lags mean the most recent year is incomplete. The corpus is English-dominant, biasing linguistic and regional perspectives (e.g., EU/eIDAS work is comparatively visible) and potentially under-representing scholarship published primarily in other languages and venues. Accordingly, our thematic signals should be interpreted as reflective of the English-indexed/English-abstract segment of the Scopus literature; extending the pipeline to multilingual corpora (e.g., via language-aware preprocessing and translation-backed validation) is left as follow-on work.

Analyses rely primarily on titles/abstracts/metadata rather than full texts, which limits capture of implementation detail and nuanced claims. Following prior evidence on abstract-based modelling [33], we interpret the resulting concepts as a high-level approximation and treat finer-grained technical omissions as a limitation to be addressed via targeted full-text validation on accessible subsets. Additionally, subject-area counts inherit the database taxonomy: articles can be multi-labelled, so tallies reflect presence rather than exclusivity and may overcount without fractional allocation. Author names and affiliations are subject to disambiguation errors, which can split or merge contributions.

Query design centred on "digital identity" and harmonised synonyms can under-capture adjacent work that does not use this phrasing. Tokenisation and normalisation choices influence which terms surface; trend lines use share of articles which contain a term, which are sensitive to variation in abstract length and editorial style. The post-2016 rise of decentralisation/ledger vocabulary may partly reflect topic salience cycles as much as deployment and this requires further investigation. Accordingly, we treat blockchain/ledger dominance as an indicative within-corpus signal that should be interpreted alongside comparator terms and validated in follow-on work using alternative corpora and controls (e.g., discipline-stratified analyses or targeted full-text/grey-literature supplementation where accessible). Citation- and subject-based summaries favour established venues and longer citation windows, disadvantaging recent contributions. Conversely, naïve year-normalisation over short windows can over-weight early citation bursts and remains sensitive to citation latency, indexing delays, and publishing seasonality. Accordingly, we treat citation totals as indicators of historical uptake and use the separate 2023–2025 stratum to surface contemporary thematic signals that may not yet be reflected in mature citation counts.

9.2. NLP and Clustering Constraints

Natural language processing and clustering are powerful for mapping large literatures, but come with limitations. Preprocessing, feature representation, and parameter choices can strongly influence results. The following key constraints are relevant to this research:

- Text preprocessing and representation—Outcomes are highly sensitive to preprocessing choices such as tokenisation, case and diacritic handling, hyphenation (e.g., block-chain vs. blockchain), and the treatment of unigrams versus multi-word expressions. Limiting analysis to abstracts compresses context, privileging editorially salient terms over operational detail. Feature representations introduce further trade-offs: bag-of-words and TF–IDF accentuate frequent but often generic tokens,

while embedding models mitigate sparsity yet inherit pre-training biases and may blur domain distinctions (e.g., wallet vs. app).

- Keyword harmonisation—Normalising near-synonyms (e.g., SSI/DID/VC), singular–plural variants, and British–American spellings helps reduce fragmentation but also risks collapsing distinct concepts (e.g., revocation vs. suspension). In addition, phrase-mining thresholds (e.g., PMI or collocation settings) influence which multi-word expressions are retained, with direct effects on observed trends and cluster formation. To improve transparency, we document the harmonisation protocol and apply automated consistency checks (e.g., idempotency and collision detection) alongside an intra-annotator test–retest agreement check for a stratified sample of mapping decisions (reported in Section 3.2).
- Term-proportion trends—Yearly proportions reflect both signal and artefact: variable abstract lengths, topic salience cycles, and uneven discipline mix by year. Without length/discipline controls, apparent rises or declines can partially reflect corpus composition rather than true thematic change.
- Clustering method and parameters—Unsupervised clustering approaches such as K-Means are highly sensitive to the choice of feature set, distance metric, initialisation, and the selected value of k. In high-dimensional spaces, sparsity can produce unstable small clusters, while flat partitions risk obscuring thematic overlap, for example between security and governance. Evaluation metrics such as topic coherence or silhouette score offer only partial guidance: they may favour easily separable clusters that are semantically shallow rather than capturing the richer, cross-cutting structure of the domain.
- Temporal windowing—Comparing 2005–2024 with 2023–2025 introduces window effects: short horizons can exaggerate sudden bursts (e.g., policy shocks, standards releases) while obscuring slower-moving themes. In addition, vocabulary drift across periods complicates the direct alignment of clusters.
- Interpretability and labelling—Assigning human-readable labels to clusters is inherently interpretive; subject taxonomies and data-driven themes only partially align. Multi-label realities (articles spanning technical, policy, and social dimensions) are flattened by single-label summaries. Although we apply explicit boundary conditions and a three-strata interpretive structure to reduce category leakage, some concepts remain inherently cross-domain in socio-technical settings; follow-on work that formalises the ontology would be able to enforce stricter separation via typed relations and constraint definitions.
- Validation and robustness—With limited "ground truth" available, validation remains challenging. External checks against subject classifications and internal diagnostics such as coherence and stability provide partial assurance but cannot guarantee semantic fidelity. Results are further affected by random-seed variance and preprocessing choices, which can shift cluster boundaries.

9.3. Thematic Blind Spots in the Literature

The survey reveals areas where evidence is thin or fragmented; addressing these would materially advance digital-identity research and practice.

- Recovery—Little comparative work on key loss/compromise, social/guardianship recovery, post-incident state repair, and survivability across wallets, issuers, and verifiers.
- Revocation—Sparse evaluation of real-time, privacy-preserving status distribution (offline use, caching, correlation risk), cross-issuer semantics, and LoA impacts.

- Interoperability—Limited cross-wallet/profile testing (VC/DID vs. eIDAS wallets), weak consensus on mandatory vs. optional features, and few reproducible conformance suites.
- Usability—Understudied design for disability, low digital literacy, multilingual settings, and vulnerable users (children, older adults); consent fatigue and mental-model mismatches persist.
- Equity—Insufficient measurement of exclusion and error across demographics (e.g., identity proofing, risk scoring), and weak links between privacy guarantees (unlinkability) and accountability/audit needs.
- Governance—Few analyses of sustainable business models for issuers/verifiers/wallet providers, liability allocation in credential flows, and procurement/assurance regimes that scale.
- Assurance—A lack of standard test oracles, traceability metrics, and multi-site benchmarks for end-to-end workflows (presentation, status, recovery), beyond single-system case studies.
- Wallet Security—Emerging attack surfaces (phishing of presentation requests, agent malware, supply-chain compromise, UI trust) lack systematic threat models and comparative mitigations.
- Offline Use—Limited evidence for low-connectivity settings (disaster response, border control, aid delivery): offline verification, key rotation, and revocation safety.
- Sector Evidence—Health, education, public-benefits, and smart-city deployments need stronger outcome studies (safety, efficacy, cost), not only architectural proposals.
- Minors—Thin treatment of age transitions, delegated authority, revocation rights, and family/organisational custodianship patterns.
- Auditability—Few designs that jointly satisfy selective disclosure/unlinkability and robust audit/compliance—especially for regulated sectors.
- AI—Early work on deepfakes and agent identity lacks principled assurance for AI-mediated proofing, presentation, and human-in-the-loop controls.
- Sustainability—Minimal life-cycle assessments (energy, latency, TCO) comparing ledger and non-ledger approaches under realistic loads.
- Global South—Over-representation of EU/US contexts; limited studies on LMIC legal/institutional constraints, trust frameworks, and cross-border service delivery.
- Legal Traceability—Few formal mappings from legal requirements to protocol properties and testable controls; compliance remains prose-level rather than machine-checkable.
- Longitudinal Outcomes—Rare multi-year studies tracking uptake, dropout, recovery events, and user outcomes across populations and sectors.

10. Future Directions

As well as addressing the broader blind spots in the digital identity literature identified in the previous section, this research can itself be extended to deliver more value towards the long-term goal of a universal digital identity. The following directions outline how the present study can be advanced and how its findings can be leveraged for greater impact.

10.1. Advancing the Present Study

This survey demonstrates the value of combining a structured corpus with computational analysis, but it also leaves room for methodological enhancement. Future work could:

- Expand corpus coverage—incorporating multilingual sources and conducting targeted full-text validation on accessible subsets (e.g., open-access samples and institutionally

licensed collections) to test whether fine-grained technical claims materially alter the high-level thematic structure derived from abstracts.
- Refine analytical methods—including the use of overlapping or hierarchical clustering, knowledge-graph–anchored semantics, and richer interpretability checks to strengthen thematic validity.
- Strengthen reproducibility—by providing open pipelines, benchmark datasets, and conformance suites that allow results to be rerun and compared as the literature evolves.

10.2. Connecting to the Universal Digital Identity Vision

Beyond methodological refinement, the findings of this survey can be mobilised towards the longer-term aim of a universal digital identity. In particular:

- Ontological development can translate recurring entities, processes, and contexts identified in the survey into formal, machine-readable structures (e.g., OWL/RDF or equivalent representations) that support semantic alignment and interoperability, including relation typing, constraint specification, and publication of reusable artefacts for downstream integration and validation.
- Cross-disciplinary vocabularies can be built by linking technical, legal, organisational, and socio-cultural concepts, helping to bridge gaps between research communities and stakeholder groups while making implicit assumptions (e.g., about governance, agency, and risk) explicit.
- Practical application of the thematic map can inform curricula, policy guidance, and system design by embedding inclusive requirements (e.g., accessibility and low-literacy settings) and trust/assurance considerations (e.g., auditability, accountability, privacy guarantees) alongside technical architectures.

11. Conclusions

We conclude by distilling the survey's main findings, reflecting on their significance for digital identity research and practice, and outlining priorities for future work towards interoperable, human-centred identity systems.

11.1. Summary of Findings

This section synthesises signals from the corpus across subjects, temporal patterns, authorship, and thematic structure. We foreground how emphasis has shifted over time—particularly towards practice and implementation—while situating recent trends against the longer-run baseline.

- Scale—Baseline corpus (2005–2024; n = 2551 publications; 2030 authors; 188 subjects; 8820 keywords), with a recent stratum (2023–2025; n = 1241) used for contemporary thematic analysis and ontology-oriented synthesis.
- Coverage—Core computing fields dominate (networks, CS, IS, AI) with substantive managerial, legal, and social strands.
- Trends—Output grows steadily, accelerating after the late 2010s; the share of "digital identity" declines as decentralisation/SSI terms gain weight—consistent with vocabulary maturation.
- Authors—Leading contributors cluster in technical areas, though several span managerial/legal/social domains, indicating both specialisation and breadth.
- Clusters (2005–24)—Long-run structure resolves into three strata: (i) technical rails (architectures, identity management, security/privacy controls); (ii) governance and institutions (policy, standards, national/EU programmes); and (iii) use and practice

(applications and socio-cultural settings). This baseline shows a balanced interplay between foundational design and policy, with applied studies secondary.

- Clusters (2023–25)—Recent work shifts towards practice and implementation: technical focus reorganises around wallet-centric trust services (VCs, status/revocation, unlinkability) and decentralised persona/presentation; governance consolidates around EU wallet/eIDAS; and applications expand in health, education, smart cities, and immersive/AI-infused environments. Standalone biometrics appear absorbed into assurance workflows and deployment pipelines rather than persisting independently.
- Ontology—Recurrent entities (actors, credentials, proofs, policies, risks, contexts) support an entity–process–context ontology that functions as a shared semantic layer for interoperable modelling and assurance. By treating context and stakeholder constraints as first-class elements (e.g., usability, accessibility, governance, sectoral deployment conditions), the framework also foregrounds inclusivity requirements and provides a structured basis for reasoning about trust across technical and institutional layers.
- Implication—The field is moving from identity-management "plumbing" to deployable wallet-based trust services and context-specific adoption, with governance and human-centred concerns shaping feasibility.

11.2. Contributions to Digital Identity Research

This section does not restate the paper's formal contributions outlined in the introduction. Instead, it reflects on the significance of the survey's findings, highlighting how they reshape our understanding of the digital identity field and where they provide added value for future research and practice. Contributions include:

1. Cross-Disciplinary Landscape—The survey demonstrates that digital identity is not confined to computer science or security, but spans at least 188 subject areas. This breadth underscores the need for integrative approaches that cut across technical, legal, organisational, and socio-cultural research communities.
2. Historical Evolution—By tracing the field from early cryptographic foundations through federated architectures to decentralised and wallet-centric models, the study clarifies how digital identity has evolved and where current momentum lies. This periodised view helps researchers position their work within longer-term trajectories rather than isolated technical debates.
3. Key Contributions—The mapping of high-impact literature and leading authors provides an entry point for scholars and practitioners to engage with foundational and contemporary debates. This strengthens the cumulative nature of digital identity research and reduces the risk of disciplinary silos.
4. Ontological Signals—Recurring entities (actors, credentials, proofs, risks, governance mechanisms) highlight the feasibility of building an ontology that supports conceptual unification across disciplines and implementation contexts. Practically, an entity–process–context framing helps (i) align semantics across heterogeneous identity stacks (supporting interoperability via shared definitions of credentials, presentation/verification workflows, and governance constraints), (ii) surface inclusion-critical requirements as explicit modelling elements (e.g., accessibility, low-literacy settings, delegated or assisted use), and (iii) connect assurance and trust questions to technical properties and institutional controls (e.g., auditability, privacy guarantees, accountability mechanisms). The survey therefore provides both an empirical basis for ontological development and a clearer pathway for operationalising it in interoperable, inclusive, and trustworthy systems. We emphasise that these structures are presented as empirically grounded fragments and scaffolding for future ontology engineering, rather than a complete machine-readable ontology artefact delivered in this work.

Together, these findings illustrate that digital identity research is simultaneously consolidating around certain technical and governance rails while fragmenting into diverse applications and contexts. The survey's value lies in making these dynamics visible, equipping the community to engage more strategically with the long-term project of developing a universal digital identity.

11.3. Closing Remarks

Our analysis indicates that digital-identity research is accelerating: annual outputs rise steadily across the period, with a marked post-2018 upswing and a recent peak (e.g., 2005–2024 counts), and the vocabulary diversifies—digital identity remains the anchor term while decentralisation/SSI terms gain share—consistent with a maturing, expanding field.

At the same time, we observe simultaneous consolidation and fragmentation. Consolidation is visible in the technical core: increasing convergence on wallet-centric trust services (verifiable credentials, status/revocation, unlinkability) and alignment with governance frameworks (e.g., eIDAS-style wallets), mirrored in recent clusters and term trends. Fragmentation arises from diverse use cases and settings: a wide subject footprint (188 areas) and recent clusters centred on sectoral deployments (health, education, cities/energy), immersive/virtual environments, and socio-cultural practices online. These contexts introduce heterogeneous requirements (assurance, usability, inclusion, policy constraints) that pull implementations in different directions even as standards solidify.

Implications of the Ontological Framework

The entity–process–context ontology provides a compact way to translate the survey's thematic structure into actionable implications for system design and evaluation:

- *Interoperability:* Shared semantics for credentials, proofs, actors, and governance constraints can reduce ambiguity between standards and implementations, enabling clearer interface contracts and supporting the development of profiles and conformance tests.
- *Inclusivity:* Modelling context explicitly supports design for diverse users and settings (e.g., accessibility and assistive use, low digital literacy, multilingual environments, sector-specific constraints), making inclusion requirements visible early rather than retrofitted.
- *Trust:* Linking technical properties (security/privacy, auditability, recovery and revocation workflows) to governance and assurance concepts helps structure trust arguments that are comparable across deployments and jurisdictions.

11.4. Potential Directions for Future Research

Accordingly, further research should prioritise comparative, cross-context evaluation of wallet/VC workflows; interoperable profiles for status, revocation, and recovery; assurance methods that couple privacy (e.g., unlinkability) with accountability; and rigorous usability and inclusion studies at scale. Shared benchmarks and conformance tests—linked to the emerging technical and governance stack—would help translate consolidation into reliable practice while accommodating the legitimate diversity of applications.

Author Contributions: The research presented in this manuscript was primarily conducted by the M.C., who was responsible for the design and execution of the study, data collection, analysis, and interpretation, as well as the drafting of the manuscript. A.M., in the capacity of a supervisor, provided overarching support and guidance throughout the research process. All authors have read and agreed to the published version of the manuscript.

Funding: A scholarship from the UK Commonwealth Scholarship Commission generously supported this research. The Commonwealth Scholarship Commission's support was purely financial and played no direct role in the study's design nor data collection, analysis, and interpretation. The findings, interpretations, and conclusions presented in this manuscript are solely the authors' responsibility and do not necessarily represent the views of the UK Commonwealth Scholarship Commission. Reference: CSC CR-2019-67.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data used in this study were obtained from the Scopus Abstract and Citation Database via programmatic access. Retrieval required an academic API key, available to registered institutional users through Elsevier. In line with journal policy, the processed datasets derived from this access are made available in the accompanying code repository referenced in the following section. Due to the intricate nature of its operational requirements, the distributed client/server architecture employed for the extraction and mining of clustered terms is not included in the provided repository at the current juncture. However, c# API baseline analysis code and clustering algorithms has been provided. Please see the github repository: https://github.com/oxford-mc/ox-identity-survey (Accessed on 10 October 2025).

Conflicts of Interest: In accordance with the guidelines outlined in the editorial policies, we hereby declare that there are no financial or non-financial competing interests associated with this manuscript. Both authors have thoroughly reviewed their respective circumstances in relation to this research and confirm that there are no conflicts of interest.

References

1. Longstaff, T.A.; Ellis, J.T.; Hernan, S.V.; Lipson, H.F.; Mcmillan, R.D.; Pesante, L.H.; Simmel, D. Security of the Internet. In *The Froehlich/Kent Encyclopedia of Telecommunications*; CRS Press: London, UK; New York, NY, USA, 1996; Volume 5, pp. 231–255.
2. Society, I. *2018 Cyber Incident and Breach Trends Report*; Internet Society: Reston, VA, USA , 2018.
3. Anderson, R.; Barton, C.; Böhme, R.; Clayton, R.; Gañán, C.; Grasso, T.; Levi, M.; Moore, T.; Vasek, M. Measuring the Changing Cost of Cybercrime. In Proceedings of the 2019 Workshop on the Economics of Information Security, Boston, MA, USA, 3–4 June 2019.
4. Harris, B.; Hunt, R. TCP/IP security threats and attack methods. *Comput. Commun.* **1999**, *22*, 885–897. [CrossRef]
5. Benantar, M. *Access Control Systems: Security, Identity Management and Trust Models*; Springer Science Business Media: Singapore, 2005.
6. Zulkarnain, S.; Idrus, S.; Cherrier, E.; Rosenberger, C.; Schwartzmann, J.J. A Review on Authentication Methods. *Aust. J. Basic Appl. Sci.* **2013**, *7*, 95–107.
7. Cameron, K. *The Laws of Identity*; Microsoft Corp: Redmond, WA, USA, 2005; pp. 8–11. [CrossRef]
8. Lyon, D. Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data Soc.* **2014**, *1*, 2053951714541861. [CrossRef]
9. Laatikainen, G.; Kolehmainen, T.; Abrahamsson, P. Self-Sovereign Identity Ecosystems: Benefits and Challenges. In Proceedings of the SCIS 2021: Proceedings of the 12th Scandinavian Conference on Information Systems, Online, 8–11 August 2021.
10. Hasselbring, W. Information system integration. *Commun. ACM* **2000**, *43*, 32–38. [CrossRef]
11. Bertino, E.; Paci, F.; Ferrini, R.; Shang, N. Privacy-preserving digital identity management for cloud computing. *IEEE Data Eng. Bull.* **2009**, *32*, 21–27
12. Josang, A.; Zomai, M.A.; Suriadi, S. Usability and privacy in identity management architectures. In *Conferences in Research and Practice in Information Technology Series*; Australian Computer Society: Sydney, Australia, 2007; Volume 68, pp. 143–152.
13. Rodrigues, R.E. Revisiting the Legal Regulation of Digital Identity in the Light of Global Implementation and Local Difference. 2011. Available online: https://scispace.com/papers/revisiting-the-legal-regulation-of-digital-identity-in-the-419jvp0wcc (accessed on 23 September 2020).
14. EPSU. The General Data Protection Regulation (GDPR) AN EPSU BRIEFING. Available online: https://www.epsu.org/sites/default/files/article/files/GDPR_FINAL_EPSU.pdf (accessed on 10 September 2024).
15. Mühle, A.; Grüner, A.; Gayvoronskaya, T.; Meinel, C. A Survey on Essential Components of a Self-Sovereign Identity. *Comput. Sci. Rev.* **2018**, *30*, 80–86. [CrossRef]

16. Toth, K.C.; Anderson-Priddy, A. Self-Sovereign Digital Identity: A Paradigm Shift for Identity. *IEEE Secur. Priv.* **2019**, *17*, 17–27. [CrossRef]
17. Birch, D.G.W. The identity vision. In *Digital Identity Management*; Routledge: London, UK, 2017; pp. 21–26.
18. Mccormack, J.I. Digital Identity Interoperability and Einnovation. Available online: http://nrs.harvard.edu/urn-3:HUL.InstRepos:2710474 (accessed on 10 December 2024).
19. Lam, W. Barriers to e-government integration. *J. Enterp. Inf. Manag.* **2005**, *18*, 511–530 [CrossRef]
20. Whitley, E.A. Trusted Digital Identity Provision: GOV.UK Verify's Federated Approach. In *CGD Policy Paper*; CGD: Boulder, CO, USA, 2018; pp. 94–120. Available online: https://eprints.lse.ac.uk/90577/ (accessed on 10 December 2024).
21. European Parliament and Council. Discover eIDAS | Shaping Europe's Digital Future. 2023. Available online: https://digital-strategy.ec.europa.eu/en/policies/discover-eidas (accessed on 10 September 2024).
22. Westin, A.F. Legal Safeguards to Insure Privacy in a Computer Society. *Commun. ACM* **1967**, *10*, 533–537. [CrossRef]
23. Chaum, D. Blind signatures for untraceable payments. In *Advances in Cryptology: Proceedings of Crypto 82*; Springer: Boston, MA, USA, 1983; pp. 199–203.
24. Clarke, R. Roger Clarke's 'Digital Persona'. 1994. Available online: https://www.rogerclarke.com/DV/DigPersona.html (accessed on 20 May 2020)
25. Zuboff, S. Surveillance Capitalism and the Challenge of Collective Action. In *New Labor Forum*; Sage Publications: Los Angeles, CA, USA, 2019; Volume 28, pp. 10–29. [CrossRef]
26. Turkle, S. *Life on the Screen Identity in the Age of the Internet*; Simon & Schuster: New York, NY, USA, 2011.
27. Boyd, D.M.; Ellison, N.B. Social network sites: Definition, history, and scholarship. *J. Comput.-Mediat. Commun.* **2007**, *13*, 210–230. [CrossRef]
28. Cavoukian, A. Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices. 2009. Available online: https://student.cs.uwaterloo.ca/~cs492/papers/7foundationalprinciples_longer.pdf (accessed on 15 July 2020).
29. Solove, D.J. *The Digital Person: Technology and Privacy in the Information Age*; NyU Press: New York, NY, USA, 2004.
30. European Union. General Data Protection Regulation (GDPR). 2016. Available online: https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed on 12 March 2024).
31. Allen, C. The Path to Self-Sovereign Identity. 2016. Available online: https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/ (accessed on 26 July 2020)
32. Westergaard, D.; Stærfeldt, H.H.; Tønsberg, C.; Jensen, L.J.; Brunak, S. A comprehensive and quantitative comparison of text-mining in 15 million full-text articles versus their corresponding abstracts. *PLoS Comput. Biol.* **2018**, *14*, e1005962. [CrossRef]
33. Syed, S.; Spruit, M. Full-Text or Abstract? Examining Topic Coherence Scores Using Latent Dirichlet Allocation. In Proceedings of the 2017 International Conference on Data Science and Advanced Analytics (DSAA), Tokyo, Japan, 19–21 October 2017; IEEE: Piscataway, NJ, USA, 2017; pp. 165–174. [CrossRef]
34. Lin, J. Is searching full text more effective than searching abstracts? *BMC Bioinform.* **2009**, *10*, 46. [CrossRef] [PubMed]
35. Divoli, A.; Wooldridge, M.A.; Hearst, M.A. Full Text and Figure Display Improves Bioscience Literature Search. *PLoS ONE* **2010**, *5*, e9619. [CrossRef] [PubMed]
36. Voisin, C.; Linden, M.; Dyke, S.O.; Bowers, S.R.; Alper, P.; Barkley, M.P.; Bernick, D.; Chao, J.; Courtot, M.; Jeanson, F.; et al. GA4GH Passport standard for digital identity and access permissions. *Cell Genom.* **2021**, *1*, 100030. [CrossRef] [PubMed]
37. Efanov, D.; Roschin, P. The all-pervasiveness of the blockchain technology. *Procedia Comput. Sci.* **2018**, *123*, 116–121. [CrossRef]
38. Bouncken, R.; Barwinski, R. *Shared Digital Identity and Rich Knowledge Ties in Global 3D Printing—A Drizzle in the Clouds?* Wiley Online Library: Hoboken, NJ, USA, 2021.
39. Takemiya, M.; Vanieiev, B. Sora identity: Secure, digital identity on the blockchain. In Proceedings of the 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), Tokyo, Japan, 23–27 July 2018.
40. Naik, N.; Jenkins, P. Governing Principles of Self-Sovereign Identity Applied to Blockchain Enabled Privacy Preserving Identity Management Systems. In Proceedings of the 2020 IEEE International Symposium on Systems Engineering (ISSE), Vienna, Austria, 12 October–12 November 2020.
41. Arner, D.; Zetzsche, D.; Buckley, R.; Barberis, J. *The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities*; Springer: Berlin/Heidelberg, Germany, 2019.
42. Zhu, X.; Badr, Y. A Survey on Blockchain-based Identity Management Systems for the Internet of Things. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018.
43. Block, J.H.; Diegel, W.; Fisch, C. How venture capital funding changes an entrepreneur's digital identity: More self-confidence and professionalism but less authenticity! *Rev. Manag. Sci.* **2024**, *18*, 2287–2319. [CrossRef]
44. Hondros, K.; Schiemer, B.; Vogelgsang, L. Beyond personal safe spaces: Creating and maintaining collective environments for meaning and identity on digital platforms. *Organization* **2023**, *30*, 809–829. [CrossRef]

45. Kavakci, E.; Kraeplin, C.R. Religious beings in fashionable bodies: The online identity construction of hijabi social media personalities. *Media Cult. Soc.* **2017**, *39*, 850–868. [CrossRef]
46. Robinson, L. The identity curation game: Digital inequality, identity work, and emotion management. *Inf. Commun. Soc.* **2018**, *21*, 661–680. [CrossRef]
47. Vivienne, S. *Digital Identity and Everyday Activism: Sharing Private Stories with Networked Publics*; Springer: Berlin/Heidelberg, Germany, 2016.
48. Manas-Viniegra, L.; Santos-Silva, D.; Liberal-Ormaechea, S. The visual-digital identity of corporate brands: A study of neuromarketing in young people from Spain and Portugal. *Tripodos* **2021**, *48*, 135–151. [CrossRef]
49. Ates, M.; Gravier, C.; Lardon, J.; Fayolle, J.; Sauviac, B. Interoperability between heterogeneous federation architectures: Illustration with SAML and WS-Federation. In Proceedings of the 2007 Third International IEEE Conference on Signal-Image Technologies and Internet-Based System, Shanghai, China, 16–18 December 2007.
50. Lee, J.H. BIDaaS: Blockchain Based ID As a Service. *IEEE Access* **2017**, *6*, 2274–2278. [CrossRef]
51. Schanzenbach, M.; Bramm, G.; Schutte, J. reclaimID: Secure, Self-Sovereign Identities using Name Systems and Attribute-Based Encryption. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing And Communications/12th IEEE International Conference on Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018. [CrossRef]
52. Cocco, L.; Tonelli, R.; Marchesi, M. Blockchain and self sovereign identity to support quality in the food supply chain. *Future Internet* **2021**, *13*, 301. [CrossRef]
53. Naik, N.; Jenkins, P. A Secure Mobile Cloud Identity: Criteria for Effective Identity and Access Management Standards. In Proceedings of the 2016 4th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), Oxford, UK, 29 March–1 April 2016.
54. Zhang, C.; Zhao, M.; Zhang, W.; Fan, Q.; Ni, J.; Zhu, L. Privacy-Preserving Identity-Based Data Rights Governance for Blockchain-Empowered Human-Centric Metaverse Communications. *IEEE J. Sel. Areas Commun.* **2024**, *42*, 963–977. [CrossRef]
55. Beck, E.N. *The Invisible Digital Identity: Assemblages in Digital Networks*; Elsevier: Amsterdam, The Netherlands, 2015.
56. Goodell, G. A Decentralised Digital Identity Architecture. *Front. Blockchain* **2019**, *2*, 17. [CrossRef]
57. Schoemaker, E.; Baslan, D.; Pon, B.; Dell, N. Identity at the margins: Data justice and refugee experiences with digital identity systems in Lebanon, Jordan, and Uganda. *Inf. Technol. Dev.* **2021**, *27*, 13–36. [CrossRef]
58. Paci, F.; Ferrini, R.; Musci, A.; Steuer, K.J.; Bertino, E. An interoperable approach to multifactor identity verification. *Computer* **2009**, *42*, 50–57. [CrossRef]
59. Munoz-Rodríguez, J.M.; Hernandez-Serrano, M.J.; Tabernero, C. Digital identity levels in older learners: A new focus for sustainable lifelong education and inclusion. *Sustainability* **2020**, *12*, 10657. [CrossRef]
60. Lim, S.Y.; Fotsing, P.T.; Almasri, A.; Musa, O.; Kiah, M.L.M.; Ang, T.F.; Ismail, R. Blockchain technology the identity management and authentication service disruptor: A survey. *Int. J. Adv. Sci. Eng. Inf. Technol.* **2018**, *8*, 1735–1745. [CrossRef]
61. Zwitter, A.J.; Gstrein, O.J.; Yap, E. Digital Identity and the Blockchain: Universal Identity Management and the Concept of the "Self-Sovereign" Individual. *Front. Blockchain* **2020**, *3*, 26. [CrossRef]
62. Rathee, T.; Singh, P. A systematic literature mapping on secure identity management using blockchain technology. *J. King Saud Univ.—Comput. Inf. Sci.* **2022**, *34*, 5782–5796. [CrossRef]
63. Grech, A.; Sood, I.; Ariño, L. Blockchain, Self-Sovereign Identity and Digital Credentials: Promise Versus Praxis in Education. *Front. Blockchain* **2021**, *4*, 616779. [CrossRef]
64. Mamun, M.A.A.; Alam, S.M.; Hossain, M.S.; Samiruzzaman, M. A Novel Approach to Blockchain-Based Digital Identity System. In *Advances in Information and Communication*; Arai, K., Kapoor, S., Bhatia, R., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 93–112.
65. Serrate-González, S.; Sánchez-Rojo, A.; Andrade-Silva, L.E.; Muñoz-Rodríguez, J.M. Onlife identity: The question of gender and age in teenagers' online behaviour. *Comunicar* **2023**, *31*, 9–19. [CrossRef]
66. Cardon, D. Identity as a Relational Strategy. 2009. Available online: https://shs.cairn.info/journal-hermes-la-revue-2009-1-page-61?lang=en (accessed on 20 September 2025).
67. Orzech, K.M.; Moncur, W.; Durrant, A.; James, S.; Collomosse, J. Digital photographic practices as expressions of personhood and identity: Variations across school leavers and recent retirees. *Vis. Stud.* **2017**, *32*, 313–328. [CrossRef]
68. Masiero, S.; Bailur, S. Digital identity for development: The quest for justice and a research agenda. *Inf. Technol. Dev.* **2021**, *27*, 1–12. [CrossRef]
69. Engeness, I. Developing teachers' digital identity: Towards the pedagogic design principles of digital environments to enhance students' learning in the 21st century. *Eur. J. Teach. Educ.* **2021**, *44*, 96–114. [CrossRef]
70. Goode, J. The digital identity divide: How technology knowledge impacts college students. *New Media Soc.* **2010**, *12*, 497–513. [CrossRef]

71. Heidari, E.; Salimi, G.; Mehrvarz, M. The influence of online social networks and online social capital on constructing a new graduate students' professional identity. *Interact. Learn. Environ.* **2023**, *31*, 214–231. [CrossRef]
72. Poole, A. Digital funds of identity: Funds of knowledge 2.0 for the digital generation. In *Conference Proceedings for IAFOR 2016*; University of Nottingham: Ningbo, China, 2016.
73. Zimmer, W.K.; McTigue, E.M.; Matsuda, N. Development and validation of the teachers' digital learning identity survey. *Int. J. Educ. Res.* **2021**, *105*, 101717. [CrossRef]
74. Zhao, G.; Di, B.; He, H. Design and Implementation of the Digital Education Transaction Subject Two-factor Identity Authentication System Based on Blockchain. In Proceedings of the 2020 22nd International Conference on Advanced Communication Technology (ICACT), PyeongChang, Republic of Korea, 16–19 February 2020.
75. Bazarhanova, A.; Smolander, K. The Review of Non-Technical Assumptions in Digital Identity Architectures. 2020. Available online: https://aisel.aisnet.org/hicss-53/st/design_responsible_system/2/ (accessed on 9 July 2024).
76. Cheesman, M. Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity. *Geopolitics* **2022**, *27*, 134–159. [CrossRef]
77. Manby, B. The Sustainable Development Goals and 'legal identity for all': 'first, do no harm'. *World Dev.* **2021**, *139*, 105343. [CrossRef]
78. Asamoah, K.O.; Xia, H.; Amofa, S.; Amankona, O.I.; Luo, K.; Xia, Q.; Gao, J.; Du, X.; Guizani, M. Zero-Chain: A Blockchain-Based Identity for Digital City Operating System. *IEEE Internet Things J.* **2020**, *7*, 10336–10346. [CrossRef]
79. Adjei, J.K.; Adams, S.; Mensah, I.K.; Tobbin, P.E.; Odei-Appiah, S. Digital identity management on social media: Exploring the factors that influence personal information disclosure on social media. *Sustainability* **2020**, *12*, 9994. [CrossRef]
80. Crowe, N.; Watts, M. When I click "ok" I become Sassy—I become a girl. Young people and gender identity: Subverting the body in massively multi-player online role-playing games. *Int. J. Adolesc. Youth* **2014**, *19*, 217–231. [CrossRef]
81. Udwan, G.; Leurs, K.; Alencar, A. Digital Resilience Tactics of Syrian Refugees in the Netherlands: Social Media for Social Support, Health, and Identity. *Soc. Media Soc.* **2020**, *6*, 2056305120915587. [CrossRef]
82. Javed, I.T.; Alharbi, F.; Bellaj, B.; Margaria, T.; Crespi, N.; Qureshi, K.N. Health-id: A blockchain-based decentralized identity management for remote healthcare. *Healthcare* **2021**, *9*, 712. [CrossRef]
83. Coats, B.; Acharya, S. Bridging electronic health record access to the cloud. In Proceedings of the Annual Hawaii International Conference on System Sciences, IEEE Computer Society, Waikoloa, HI, USA, 6–9 January 2014; pp. 2948–2957. [CrossRef]
84. Rohner, P. Identity management for health professionals: A method for the integration of responsibility, organization, and IT. *Bus. Inf. Syst. Eng.* **2013**, *5*, 17–33. [CrossRef]
85. Kaushik, S.; Gandhi, C. Ensure hierarchal identity based data security in cloud environment. *Int. J. Cloud Appl. Comput. (IJCAC)* **2019**, *9*, 21–36. [CrossRef]
86. Niezen, R. Digital Identity: The Construction of Virtual Selfhood in the Indigenous Peoples' Movement. *Comp. Stud. Soc. Hist.* **2005**, *47*, 532–551. [CrossRef]
87. Mitrushchenkova, A.N. Personal Identity in the Metaverse: Challenges and Risks. *Kutafin Law Rev.* **2022**, *9*, 793–817. [CrossRef]
88. Ruiu, P.; Nitti, M.; Pilloni, V.; Cadoni, M.; Grosso, E.; Fadda, M. Metaverse & Human Digital Twin: Digital Identity, Biometrics, and Privacy in the Future Virtual Worlds. *Multimodal Technol. Interact.* **2024**, *8*, 48. [CrossRef]
89. Soldatova, G.U.; Chigarkova, S.V.; Ilyukhina, S.N. Real-self and virtual-self: Identity matrices of adolescents and adults. *Cult.-Hist. Psychol.* **2022**, *18*, 27–37.
90. Mir, U.; Kar, A.K.; Gupta, M.P. AI-enabled digital identity—Inputs for stakeholders and policymakers. *J. Sci. Technol. Policy Manag.* **2022**, *13*, 514–541. [CrossRef]
91. Dunphy, P.; Petitcolas, F.A.P. A First Look at Identity Management Schemes on the Blockchain. *IEEE Secur. Priv.* **2018**, *16*, 20–29. [CrossRef]
92. Rouhani, S.; Deters, R. Security, performance, and applications of smart contracts: A systematic survey. *IEEE Access* **2019**, *7*, 50759–50779. [CrossRef]
93. Liu, Y.; He, D.; Obaidat, M.S.; Kumar, N.; Khan, M.K.; Choo, K.K.R. Blockchain-based identity management systems: A review, 2020. *J. Netw. Comput. Appl.* **2020**, *166*, 102731. [CrossRef]
94. Sarma, A.C.; Girão, J. Identities in the future internet of things. *Wirel. Pers. Commun.* **2009**, *49*, 353–363. [CrossRef]
95. Sullivan, C.; Burger, E. E-residency and blockchain. *Comput. Law Secur. Rev.* **2017**, *33*, 470–481. [CrossRef]
96. Satybaldy, A.; Nowostawski, M.; Ellingsen, J. Self-Sovereign Identity Systems Evaluation framework. In *IFIP International Summer School on Privacy and Identity Management 19 August 2019*; Springer International Publishing: Cham, Switzerland, 2020.
97. Xu, Q.; Jing, Y. Ambient identity construction via massive anonymous danmu comments. *Lang. Sci.* **2024**, *104*, 101631. [CrossRef]
98. Dieye, M.; Valiorgue, P.; Gelas, J.P.; Diallo, E.H.; Ghodous, P.; Biennier, F.; Peyrol, E. A Self-Sovereign Identity Based on Zero-Knowledge Proof and Blockchain. *IEEE Access* **2023**, *11*, 49445–49455. [CrossRef]
99. Sharif, A.; Ranzi, M.; Carbone, R.; Sciarretta, G.; Marino, F.A.; Ranise, S. The eIDAS Regulation: A Survey of Technological Trends for European Electronic Identity Schemes. *Appl. Sci.* **2022**, *12*, 12679. [CrossRef]

100. Hert, P.D. Identity management of e-ID, privacy and security in Europe. A human rights view. *Inf. Secur. Tech. Rep.* **2008**, *13*, 71–75. [CrossRef]
101. Sperfeldt, C. Legal identity in the sustainable development agenda: Actors, perspectives and trends in an emerging field of research. *Int. J. Hum. Rights* **2022**, *26*, 217–238. [CrossRef]
102. Ayed, G.B.; Ghernaouti-Hélie, S. Privacy Requirements Specification for Digital Identity Management Systems Implementation: Towards a Digital Society of Privacy. In Proceedings of the 2011 International Conference for Internet Technology and Secured Transactions, Abu Dhabi, United Arab Emirites, 11–14 December 2011; IEEE: Piscataway, NJ, USA, 2011.
103. Fernandez-Marcial, V.; Gonzalez-Solar, L. Research promotion and digital identity: The case of the Universidade da Coruña. *Prof. Inf.* **2015**, *24*, 656–664. [CrossRef]
104. Robles-Carrillo, M. Digital identity: An approach to its nature, concept, and functionalities. *Int. J. Law Inf. Technol.* **2024**, *32*, eaae019. [CrossRef]
105. Sullivan, C. Blockchain-based identity: The advantages and disadvantages. In *Blockchain and the Public Sector: Theories, Reforms, and Case Studies*; Springer: Cham, Switzerland, 2021; pp. 197–218.
106. Al-Khouri, A.M. Digital identity: Transforming GCC economies. *Innov. Manag. Policy Pract.* **2014**, *16*, 184–194. [CrossRef]
107. Rogova, N.; Matta, S. The role of identity in digital consumer behavior: A conceptual model and research propositions based on gender. *AMS Rev.* **2023**, *13*, 55–70. [CrossRef]
108. Coteli, S. The Impact of New Media on The Forms of Culture: Digital Identity and Digital Culture. *Online J. Commun. Media Technol.* **2019**, *9*, e201911. [CrossRef]
109. Wang, F.; Filippi, P.D. Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion. *Front. Blockchain* **2019**, *2*, 28. [CrossRef]
110. Mir, U.B.; Kar, A.K.; Dwivedi, Y.K.; Gupta, M.P.; Sharma, R.S. Realizing Digital Identity in Government: Prioritizing design and implementation objectives for Aadhaar in India. *Gov. Inf. Q.* **2020**, *37*, 101442. [CrossRef]
111. Masiero, S.; Arvidsson, V. Degenerative outcomes of digital identity platforms for development. *Inf. Syst. J.* **2021**, *31*, 903–928. [CrossRef]
112. Shuaib, M.; Hassan, N.H.; Usman, S.; Alam, S.; Bhatia, S.; Agarwal, P.; Idrees, S.M. Land Registry Framework Based on Self-Sovereign Identity (SSI) for Environmental Sustainability. *Sustainability* **2022**, *14*, 5400. [CrossRef]
113. Feulner, S.; Sedlmeir, J.; Schlatt, V.; Urbach, N. Exploring the use of self-sovereign identity for event ticketing systems. *Electron. Mark.* **2022**, *32*, 1759–1777. [CrossRef] [PubMed]
114. Lou, J.; Han, N.; Wang, D.; Pei, X. Effects of Mobile Identity on Smartphone Symbolic Use: An Attachment Theory Perspective. *Int. J. Environ. Res. Public Health* **2022**, *19*, 14036. [CrossRef] [PubMed]
115. Lips, M. Rethinking citizen-government relationships in the age of digital identity: Insights from research. *Inf. Polity* **2010**, *15*, 273–289. [CrossRef]
116. Lips, A.M.B.; Taylor, J.A.; Organ, J. Managing citizen identity information in e-government service relationships in the UK: The emergence of a surveillance state or a service state? *Public Manag. Rev.* **2009**, *11*, 833–856. [CrossRef]
117. Sullivan, C.; Tyson, S. A global digital identity for all: The next evolution. *Policy Des. Pract.* **2023**, *6*, 433–445. [CrossRef]
118. Seltsikas, P.; O'Keefe, R.M. Expectations and outcomes in electronic identity management: The role of trust and public value. *Eur. J. Inf. Syst.* **2010**, *19*, 93–103. [CrossRef]
119. Zloteanu, M.; Harvey, N.; Tuckett, D.; Livan, G. Digital identity: The effect of trust and reputation information on user judgement in the sharing economy. *PLoS ONE* **2018**, *13*, e0209071. [CrossRef]
120. L'Amrani, H.; Berroukech, B.E.; Idrissi, Y.E.B.E.; Ajhoun, R. Identity management systems: Laws of identity for models7 evaluation. In Proceedings of the Colloquium in Information Science and Technology, CIST, Tangier, Morocco, 24–26 October 2016; Institute of Electrical and Electronics Engineers Inc.: Piscataway, NJ, USA, 2016; pp. 736–740. [CrossRef]
121. Kumar, V.; Pradhan, P. Trust management: Social vs. Digital identity. *Int. J. Serv. Sci. Manag. Eng. Technol.* **2020**, *11*, 26–44. [CrossRef]
122. Jennings, B.; Finkelstein, A. Digital Identity and Reputation in the Context of a Bounded Social Ecosystem. In *Business Process Management Workshops (BPM 2008 International Workshops), Milan, Italy, 1–4 September 2008*; Ardagna, D., Mecella, M., Yang, J., Eds.; Lecture Notes in Business Information Processing; Springer: Berlin/Heidelberg, Germany, 2009; Volume 17, pp. 687–697. [CrossRef]
123. Xu, L.; Chen, L.; Gao, Z.; Chang, Y.; Iakovou, E.; Shi, W. Binding the Physical and Cyber Worlds: A Blockchain Approach for Cargo Supply Chain Security Enhancement. In Proceedings of the 2018 IEEE International Symposium on Technologies for Homeland Security (HST), Woburn, MA, USA, 23–24 October 2018.
124. Ates, M.; Ravet, S.; Ahmat, A.M.; Fayolle, J. An Identity-Centric Internet: Identity in the Cloud, Identity as a Service and other delights. In Proceedings of the 2011 Sixth International Conference on Availability, Reliability and Security, Vienna, Austria, 22–26 August 2011.
125. Wood, P. Implementing identity management security—An ethical hacker's view. *Netw. Secur.* **2005**, *2005*, 12–15. [CrossRef]

126. Zhu, X.; Badr, Y. Identity management systems for the internet of things: A survey towards blockchain solutions. *Sensors* **2018**, *18*, 4215. [CrossRef]
127. Yin, J.; Xiao, Y.; Pei, Q.; Ju, Y.; Liu, L.; Xiao, M.; Wu, C. SmartDID: A Novel Privacy-Preserving Identity Based on Blockchain for IoT. *IEEE Internet Things J.* **2023**, *10*, 6718–6732. [CrossRef]
128. Sule, M.J.; Zennaro, M.; Thomas, G. Cybersecurity through the lens of Digital Identity and Data Protection: Issues and Trends. *Technol. Soc.* **2021**, *67*, 101734. [CrossRef]
129. Stokkink, Q.; Ishmaev, G.; Epema, D.; Pouwelse, J. A truly self-sovereign identity system. In Proceedings of the Conference on Local Computer Networks, LCN, Edmonton, AB, Canada, 4–7 October 2021; IEEE Computer Society: Piscataway, NJ, USA, 2021; pp. 81–89. [CrossRef]
130. Beduschi, A. Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. *Big Data Soc.* **2019**, *6*, 2053951719855091. [CrossRef]
131. Fisch, C.; Block, J.H. How does entrepreneurial failure change an entrepreneur's digital identity? Evidence from Twitter data. *J. Bus. Ventur.* **2021**, *36*, 106015. [CrossRef]
132. Feher, K. Digital identity and the online self: Footprint strategies - An exploratory and comparative research study. *J. Inf. Sci.* **2021**, *47*, 192–205. [CrossRef]
133. Cho, V.; Jimerson, J.B. Managing digital identity on Twitter: The case of school administrators. *Educ. Manag. Adm. Leadership.* **2017**, *45*, 884–900. [CrossRef]
134. Ruan, B.; Yilmaz, Y.; Lu, D.; Lee, M.; Chan, T.M. Defining the digital self: A qualitative study to explore the digital component of professional identity in the health professions. *J. Med. Internet Res.* **2020**, *22*, 21416. [CrossRef]
135. Doring, N.; Bhana, D.; Albury, K. Digital sexual identities: Between empowerment and disempowerment. *Curr. Opin. Psychol.* **2022**, *48*, 101466. [CrossRef]
136. Rieger, A.; Roth, T.; Sedlmeir, J.; Weigl, L.; Fridgen, G. Not yet another digital identity. *Nat. Hum. Behav.* **2022**, *6*, 3. [CrossRef]
137. Han, H.; Hawken, S. Introduction: Innovation and identity in next-generation smart cities. *City Cult. Soc.* **2018**, *12*, 1–4. [CrossRef]
138. Bussone, A.; Kasadha, B.; Stumpf, S.; Durrant, A.C.; Tariq, S.; Gibbs, J.; Lloyd, K.C.; Bird, J. Trust, Identity, Privacy, and Security Considerations for Designing a Peer Data Sharing Platform between People Living with HIV. *Proc. ACM Hum.-Comput. Interact.* **2020**, *4*, 1–27. [CrossRef]
139. Code, J. Agency and identity in social media. In *Digital Identity and Social Media*; IGI Global: Hershey, PA, USA, 2012; pp. 37–57. [CrossRef]
140. Sarav, S.; Kerikmae, T. E-residency: A cyberdream embodied in a digital identity card? In *The Future of Law and eTechnologies*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 57–79.
141. Weitzberg, K.; Cheesman, M.; Martin, A.; Schoemaker, E. Between surveillance and recognition: Rethinking digital identity in aid. *Big Data Soc.* **2021**, *8*, 20539517211006744. [CrossRef]
142. Allison, A.; Currall, J.; Moss, M.; Stuart, S. Digital Identity Matters. *J. Am. Soc. Inf. Sci. Technol.* **2005**, *56*, 364–372. [CrossRef]
143. Liu, M.D.; Chen, Z.N.; Shi, Y.J.; Tang, L.T.; Cao, D. Research progress of blockchain in data security. *Chin. J. Comput* **2021**, *44*, 1–27.
144. Emanuel, L.; Fraser, D.S. Exploring physical and digital identity with a teenage cohort. In Proceedings of the 2014 Conference on Interaction Design and Children, Aarhus, Denmark, 17–20 June 2014; ACM International Conference Proceeding Series; Association for Computing Machinery: New York, NY, USA, 2014; pp. 67–76. [CrossRef]
145. Bertino, E.; Takahashi, K. *Proceedings of the 4th ACM Workshop on Digital Identity Management: 2008, Alexandria, VA, USA, 31 October 2008*; Association for Computing Machinery: New York, NY, USA, 2008; p. 105. Available online: https://dl.acm.org/doi/proceedings/10.1145/1456424 (accessed on 8 January 2026). [CrossRef]
146. Gulotta, R.; Faste, H.; Mankoff, J. Curation, Provocation, and Digital Identity: Risks and Motivations for Sharing Provocative Images Online. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Austin, TX, USA, 5–10 May 2012.
147. Yang, X.; Li, W. A zero-knowledge-proof-based digital identity management scheme in blockchain. *Comput. Secur.* **2020**, *99*, 102050. [CrossRef]
148. Laurent, M.; Denouël, J.; Levallois-Barth, C.; Waelbroeck, P. Digital Identity. In *Digital Identity Management*; Laurent, M., Bouzefrane, S., Eds.; Elsevier (ISTE Press): Amsterdam, The Netherlands, 2015; pp. 1–45. [CrossRef]
149. Grüner, A.; Mühle, A.; Gayvoronskaya, T.; Meinel, C. A comparative analysis of trust requirements in decentralized identity management. In *Proceedings of the International Conference on Advanced Information Networking and Applications (AINA 2019)*; Springer International Publishing: Cham, Switzerland, 2019; pp. 200–213.
150. Kim, E.; Cho, Y.S.; Kim, B.; Ji, W.; Kim, S.H.; Woo, S.S.; Kim, H. Can we create a cross-domain federated identity for the industrial internet of things without google? *IEEE Internet Things Mag.* **2020**, *3*, 82–87. [CrossRef]
151. Buccafurri, F.; Fotia, L.; Lax, G.; Mammoliti, R. Enhancing public digital identity system (SPID) to prevent information leakage. In *Proceedings of the Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer: Berlin/Heidelberg, Germany, 2015; Volume 9265, pp. 57–70. [CrossRef]

152. Gill, B.C.; Zampini, A.M.; Mehta, N.B. Digital identity: Develop one before you're given one. *Urology* **2015**, *85*, 1219–1223. [CrossRef]
153. Careja, A.C.; Tapus, N. Digital Identity Using Blockchain Technology. *Procedia Comput. Sci.* **2023**, *221*, 1074–1082. [CrossRef]
154. Nita, S.L.; Mihailescu, M.I. A Novel Authentication Scheme Based on Verifiable Credentials Using Digital Identity in the Context of Web 3.0. *Electronics* **2024**, *13*, 1137. [CrossRef]
155. Kingo, T.; Aranha, D.F. User-centric security analysis of MitID: The Danish passwordless digital identity solution. *Comput. Secur.* **2023**, *132*, 103376. [CrossRef]
156. Heiss, J.; Muth, R.; Pallas, F.; Tai, S. Non-disclosing Credential On-chaining for Blockchain-Based Decentralized Applications. In *Service-Oriented Computing (ICSOC 2022), Seville, Spain, 29 November–2 December 2022*; Troya, J., Medjahed, B., Piattini, M., Yao, L., Fernández, P., Ruiz-Cortés, A., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2022; Volume 13740, pp. 351–368. [CrossRef]
157. Lan, F.; Jiang, Y. Optimization Exploration of Digital Identity Authentication Algorithm Based on Blockchain. *Appl. Math. Nonlinear Sci.* **2024**, *9*, 20241704–20241716. [CrossRef]
158. Wu, H.; Zhang, W. Digital identity, privacy security, and their legal safeguards in the Metaverse. *Secur. Saf.* **2023**, *2*, 2023011. [CrossRef]
159. Wang, S.; Wang, W. A review of the application of digital identity in the Metaverse. *Secur. Saf.* **2023**, *2*, 2023009. [CrossRef]
160. Sanabria, E.M.Q.; Avellaneda, J.C.P.; Zuasnabar, E.E.B.; García, A.M.H.; Mincami, L.D.M.; Giron, H.R.; Quispe, Y.S. Blockchain Technology in Digital Identity Management and Verification. *Data Metadata* **2024**, *3*, 326. [CrossRef]
161. Hilowle, M.; Yeoh, W.; Grobler, M.; Pye, G.; Jiang, F. Users' Adoption of National Digital Identity Systems: Human-Centric Cybersecurity Review. *J. Comput. Inf. Syst.* **2023**, *63*, 1264–1279. [CrossRef]
162. Hilowle, M.; Yeoh, W.; Grobler, M.; Pye, G.; Jiang, F. Improving National Digital Identity Systems Usage: Human-Centric Cybersecurity Survey. *J. Comput. Inf. Syst.* **2024**, *64*, 820–834. [CrossRef]
163. Paier, M.; Eeden, R.V.; Miculan, M. Formal Analysis of Multi-Factor Authentication Schemes in Digital Identity Cards. In *Proceedings of the International Conference on Software Engineering and Formal Methods*; Springer: Cham, Switzerland, 2024; pp. 423–440.
164. Boldrin, L. A Model-Theoretic Approach to Digital Identity. 2025. Available online: https://ceur-ws.org/Vol-3968/invited1.pdf (accessed on 22 September 2025).
165. Rivera, J.J.D.; Muhammad, A.; Song, W.C. Securing Digital Identity in the Zero Trust Architecture: A Blockchain Approach to Privacy-Focused Multi-Factor Authentication. *IEEE Open J. Commun. Soc.* **2024**, *5*, 2792–2814. [CrossRef]
166. Wang, F.; Gai, Y.; Zhang, H. Blockchain user digital identity big data and information security process protection based on network trust. *J. King Saud Univ.—Comput. Inf. Sci.* **2024**, *36*, 102031. [CrossRef]
167. Comb, M.; Martin, A. Mining digital identity insights: Patent analysis using NLP. *EURASIP J. Inf. Secur.* **2024**, *2024*, 21. [CrossRef]
168. Buccafurri, F.; Lax, G.; Russo, A. Allowing Privacy-Preserving Fog Computing with Digital Identity Assurance in Remote Clinical Services. *Electron. Gov. Int. J.* **2023**, *19*, 185–201. [CrossRef]
169. Song, Z.; Yan, E.; Song, J.; Jiang, R.; Yu, Y.; Chen, T. A Blockchain-Based Digital Identity System with Privacy, Controllability, and Auditability. *Arab. J. Sci. Eng.* **2025**, *50*, 7027–7051. [CrossRef]
170. Jena, S.K.; Barik, R.C.; Priyadarshini, R. A systematic state-of-art review on digital identity challenges with solutions using conjugation of IOT and blockchain in healthcare. *Internet Things* **2024**, *25*, 101111. [CrossRef]
171. Lareki, A.; Altuna, J.; de Morentin, J.I.M. Fake digital identity and cyberbullying. *Media Cult. Soc.* **2023**, *45*, 338–353. [CrossRef]
172. Masiero, S. Digital identity as platform-mediated surveillance. *Big Data Soc.* **2023**, *10*, 20539517221135176. [CrossRef]
173. Giannini, T.; Bowen, J.P. Global Cultural Conflict and Digital Identity: Transforming Museums. *Heritage* **2023**, *6*, 1986–2005. [CrossRef]
174. Block, J.H.; Fisch, C.; Diegel, W. Schumpeterian entrepreneurial digital identity and funding from venture capital firms. *J. Technol. Transf.* **2024**, *49*, 119–157. [CrossRef]
175. Matas, P.M.; Gil, Í. Visual communication and narrative discourse in social networks: Emma watson's digital identity on instagram. *Vis. Rev. Int. Vis. Cult. Rev./Rev. Int. Cult. Vis.* **2024**, *16*, 211–224. [CrossRef]
176. Masitoh, F.; Cahyono, B.Y.; Suryati, N.; Suhartoyo, E. Pre-service EFL teachers' identity construction in relation to digital gamification: A social theory of learning perspective. *JALT CALL J.* **2023**, *19*, 369–393. [CrossRef]
177. Li, S.; Wu, J.G.; Bian, J.; Ding, Z.; Sun, Y. Understanding Digital Identity during the Pandemic: An Investigation of Two Chinese Spanish Teachers. *Sustainability* **2023**, *15*, 1208. [CrossRef]
178. Puspitasari, D.A.; Karlina, Y.; Hernina, H.; Kurniawan, K.; Sutejo, S.; Danardana, A.S. Language Choices and Digital Identity of High School Student Text Messages in the New Capital City of Indonesia: Implication for Language Education. *Int. J. Lang. Educ.* **2024**, *8*, 162–184. [CrossRef]
179. Degen, K.; Teubner, T. Wallet wars or digital public infrastructure? Orchestrating a digital identity data ecosystem from a government perspective. *Electron. Mark.* **2024**, *34*, 50. [CrossRef]

180. Schwalm, S. The possible impacts of the eIDAS 2.0 digital identity approach in Germany and Europe. In *Proceedings of the Lecture Notes in Informatics (LNI), Proceedings—Series of the Gesellschaft fur Informatik (GI)*; Gesellschaft fur Informatik (GI): Deutschland, Germany, 2023; Volume P-335, pp. 109–120. [CrossRef]
181. Martinez, G.T. Disability in the European Digital Identity Wallet (EUDI wallet): An opportunity to improve accessibility and efficient contracts. *Onati Socio-Legal Ser.* **2025**, *15*, 890–915. [CrossRef]
182. Ibor, A.; Hooper, M.; Maple, C.; Crowcroft, J.; Epiphaniou, G. Considerations for trustworthy cross-border interoperability of digital identity systems in developing countries. *AI Soc.* **2025**, *40*, 2729–2750. [CrossRef] [PubMed]
183. Inza, J. The European Digital Identity Wallet as Defined in the EIDAS 2 Regulation. In *Governance and Control of Data and Digital Economy in the European Single Market: Legal Framework for New Digital Assets, Identities and Data Spaces*; Springer Nature: Cham, Switzerland, 2025; pp. 433–452.
184. Rafajac, O.; Jakupovic, A. *Integral Communication and Digital Identity*; Springer Nature: Berlin/Heidelberg, Germany, 2023.