Engineering and Technology Journal e-ISSN: 2456-3358

Volume 10 Issue 02 February-2025, Page No.- 3798-3804

DOI: 10.47191/etj/v10i02.09, I.F. – 8.482

Blockchain's Transformative Potential in Securing Digital Identities and Personal Data

Olanrewaju Oluwaseun Ajayi[1], Chisom Elizabeth Alozie[2], Olumese Anthony Abieba[3]

[1,2]University of the Cumberlands

[3]Abeam Consulting USA

ABSTRACT: This review paper explores the transformative potential of blockchain technology in securing digital identities and personal data. It examines various blockchain applications, including identity verification, self-sovereign identity, and decentralized authentication mechanisms. Despite scalability issues, interoperability concerns, and regulatory hurdles, ongoing developments promise to overcome these obstacles. Future directions in blockchain technology include scalability solutions, interoperability standards, and privacy-enhancing technologies. Additionally, integration with AI and machine learning presents opportunities for enhancing identity verification processes. Collaboration between industry stakeholders and policymakers is crucial for shaping regulatory frameworks that promote innovation while safeguarding privacy rights. Overall, blockchain technology offers a decentralized and transparent approach to digital identity management and personal data security, with significant implications for empowering individuals and enhancing trust in the digital ecosystem.

KEYWORDS: Blockchain, Digital Identity, Personal Data Security, Self-sovereign Identity, Decentralized Authentication, Privacy-enhancing Technologies

1. INTRODUCTION

In the digital landscape of today, where our lives are increasingly intertwined with online platforms and services, the security of our digital identities and personal data has become paramount. Every digital interaction, whether logging into social media accounts, making online purchases, or accessing healthcare records, leaves behind a trail of personal information susceptible to exploitation by malicious actors. Protecting digital identities and personal data has emerged as a critical challenge in the digital age.

Digital identities encompass the digital representations of individuals, encompassing a wide array of attributes, including usernames, passwords, biometric data, and more (Knight & Saxby, 2014; Zwitter, Gstrein, & Yap, 2020). Personal data, on the other hand, comprises any information that can be used to identify an individual, such as name, address, financial details, and browsing history. Both digital identities and personal data are vulnerable to various threats, including identity theft, data breaches, surveillance, and unauthorized access. The consequences of such breaches can range from financial loss and reputational damage to potential harm to individuals' safety and privacy (Chua, Ooi, & Herbland, 2021; Tene & Polonetsky, 2012).

The significance of securing digital identities and personal data cannot be overstated, as they form the foundation of trust in the digital ecosystem. Individuals must have confidence that their identities are protected and that their data is handled responsibly by the organizations and platforms they interact with. However, achieving this level of security poses numerous challenges. Traditional identity management and data security methods, such as centralized databases and password-based authentication, are inherently vulnerable to attacks. Moreover, the increasing volume and complexity of digital transactions exacerbate these challenges, making it difficult for individuals and organizations to safeguard their digital identities and personal data effectively.

Blockchain technology has emerged as a promising solution to the security and privacy concerns surrounding digital identities and personal data. Blockchain is a decentralized and distributed ledger technology that enables secure, transparent, and immutable record-keeping. Key principles of blockchain include decentralization, cryptographic security, consensus mechanisms, and immutability (Bernabe, Canovas, Hernandez-Ramos, Moreno, & Skarmeta, 2019). By leveraging these principles, blockchain offers a paradigm shift in how digital identities and personal data can be managed and secured, providing individuals with greater control over their information and reducing reliance on centralized authorities (Zhu & Badr, 2018).

In light of the significant challenges facing digital identity management and personal data security, this research paper contends that blockchain technology holds transformative potential in addressing these concerns. By decentralizing trust, enhancing security, and empowering individuals with greater control over their digital identities and personal data, blockchain can revolutionize how we perceive and manage

identity in the digital age. By exploring blockchain's principles, applications, and challenges, this paper aims to provide insights into how blockchain can shape the future of digital identity and personal data security.

2. LITERATURE REVIEW

In the contemporary digital landscape, digital identities and personal data are pivotal in shaping interactions, transactions, and relationships across various online platforms and services. Understanding the nature of digital identities and the significance of safeguarding personal data is essential for comprehending the challenges and imperatives in ensuring robust security measures in the digital realm.

2.1. Definition and Importance of Digital Identities and Personal Data

Digital identities encompass the digital representations of individuals within the digital ecosystem. These identities are comprised of various attributes, including but not limited to usernames, passwords, biometric data, social security numbers, and email addresses. They serve as how individuals authenticate themselves and access online services, ranging from social media platforms and e-commerce websites to banking and healthcare portals (Baier, Zirpins, & Lamersdorf, 2003; Mueller, Park, Lee, & Kim, 2006).

Personal data, however, refers to any information that can be used to identify an individual. This includes sensitive information such as name, address, date of birth, financial details, medical records, browsing history, and more (Ana Beduschi, 2019). Personal data is the cornerstone of personalized services and targeted marketing strategies in the digital economy, making it highly valuable to legitimate businesses and malicious actors seeking to exploit vulnerabilities for financial gain or other nefarious purposes (A Beduschi, Cinnamon, Langford, Luo, & Owen, 2017; Laurent, Denouël, Levallois-Barth, & Waelbroeck, 2015).

The importance of digital identities and personal data lies in their role as the gateway to online activities and services. They enable individuals to engage in digital transactions, communicate with others, and access essential services conveniently. However, the proliferation of digital identities and the extensive collection and utilization of personal data have also raised concerns about privacy, security, and potential misuse or abuse.

2.2. Overview of Current Methods and Technologies Used for Securing Digital Identities and Personal Data

In response to the growing threats posed by cyberattacks, data breaches, and identity theft, various methods and technologies have been developed to secure digital identities and personal data. These include (Jain, 2007; Luevanos, Elizarraras, Hirschi, & Yeh, 2017; Sullivan, 2018; Thomas et al., 2017):

i. Password-based Authentication: Historically, passwords have been the primary method of authenticating users and granting access to digital services. However, passwords are prone to weaknesses such as brute force attacks, phishing, and password reuse, making them susceptible to exploitation by cybercriminals.

ii. Multi-factor Authentication (MFA): MFA enhances security by requiring users to provide multiple forms of identification, such as a password, a one-time passcode sent to a mobile device, or biometric authentication (e.g., fingerprint or facial recognition). While MFA offers an additional layer of security, it is not immune to social engineering attacks or sophisticated cyber threats.

iii. Encryption: Encryption technologies, such as Secure Socket Layer (SSL) and Transport Layer Security (TLS), are used to secure data transmission over the internet, ensuring that sensitive information remains confidential and protected from interception or eavesdropping.

iv. Identity and Access Management (IAM): IAM solutions help organizations manage user identities, roles, and permissions, ensuring that only authorized individuals can access specific resources or data. IAM systems employ role-based access control (RBAC) and attribute-based access control (ABAC) to enforce security policies and mitigate the risk of unauthorized access.

Despite the widespread adoption of security measures and technologies, existing systems for securing digital identities and personal data are not without vulnerabilities and shortcomings. Centralized databases, commonly used to store and manage user information, present single points of failure and are attractive targets for cybercriminals seeking to steal large volumes of sensitive data in a single breach. Moreover, traditional authentication methods such as passwords are susceptible to various attack vectors, including password guessing, credential stuffing, and phishing attacks.

Furthermore, the commodification and monetization of personal data by tech companies and data brokers raise concerns about privacy infringement and the erosion of user consent and control over their information. The pervasive collection and aggregation of personal data across multiple platforms and services create extensive digital footprints that can be exploited for profiling, targeting, and surveillance purposes without adequate transparency or accountability mechanisms (Bietti, 2019).

In light of these vulnerabilities and shortcomings, there is an urgent need for improved security measures and privacy protection mechanisms in the digital realm. As digital interactions become increasingly integral to everyday life, individuals must have confidence that their digital identities and personal data are safeguarded against unauthorized access, misuse, and exploitation (Suzor, 2019). Enhanced security measures, such as biometric authentication, blockchain-based identity solutions, and zero-trust security

architectures, offer promising avenues for bolstering the resilience of digital identity and data security systems. Similarly, regulatory frameworks such as the General Data Protection Regulation (GDPR) aim to empower individuals with greater control over their data and hold organizations accountable for data protection practices (Windley, 2005).

In summary, the evolving threat landscape and the growing ubiquity of digital technologies underscore the imperative for continuous innovation and collaboration in developing robust security measures and privacy-enhancing technologies that uphold the integrity, confidentiality, and autonomy of digital identities and personal data in the digital age.

3. BLOCKCHAIN TECHNOLOGY: PRINCIPLES AND FEATURES

Blockchain technology has garnered significant attention and acclaim for its potential to revolutionize various industries by offering unprecedented levels of security, transparency, and decentralization. Understanding blockchain's core principles and features is crucial for grasping its transformative potential in securing digital identities and personal data.

At its essence, blockchain is a distributed ledger technology that enables peer-to-peer transactions in a secure, transparent, and immutable manner. Unlike traditional centralized systems where data is stored and controlled by a single authority, blockchain operates on a decentralized network of computers (nodes), each maintaining a copy of the ledger. This decentralized nature eliminates the need for intermediaries and central authorities, thereby reducing the risk of single points of failure and enhancing resilience against cyberattacks.

3.1. Key Components

i. Blocks: In blockchain, data is grouped into blocks, each containing a collection of transactions. These blocks are linked chronologically to form a chain, hence the term "blockchain." Each block contains a cryptographic hash of the previous block, ensuring the integrity and immutability of the entire chain (Xu, Pautasso, Zhu, Lu, & Weber, 2018).

ii. Consensus Mechanisms: Consensus mechanisms are protocols that enable nodes in a blockchain network to agree on the validity of transactions and maintain the integrity of the ledger without the need for a central authority. Popular consensus mechanisms include Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS), each with its own set of advantages and trade-offs in terms of security, scalability, and energy efficiency (Wang et al., 2019).

iii. Smart Contracts: Smart contracts are self-executing contracts with the terms of the agreement directly written into code. These contracts automatically execute and enforce predefined rules and conditions when specific conditions are met, eliminating the need for intermediaries and facilitating trustless transactions. Smart contracts are typically deployed on blockchain platforms such as Ethereum and enable a wide range of applications, including decentralized finance (DeFi), supply chain management, and decentralized autonomous organizations (DAOs).

3.2. Overview of Different Types of Blockchains

Blockchain networks can be categorized into three main types based on their accessibility and governance:

i. Public Blockchains: Public blockchains, such as Bitcoin and Ethereum, are open and permissionless networks where anyone can participate, transact, and validate transactions. These networks are characterized by their decentralized nature and censorship resistance, making them ideal for applications requiring a high degree of trustlessness and transparency (Alston, Law, Murtazashvili, & Weiss, 2021; Taskinsoy, 2019).

ii. Private Blockchains: Private blockchains are permissioned networks where access and participation are restricted to authorized entities. Unlike public blockchains, which prioritize decentralization and transparency, private blockchains prioritize privacy, scalability, and control. These networks are commonly used for supply chain management, identity verification, and inter-organizational collaboration applications in enterprise settings (Huang, Chung, Dong, Luo, & Kang, 2019; Mohan, 2019).

iii. Consortium Blockchains: Consortium blockchains, also known as federated blockchains, are semi-decentralized networks governed by a consortium or group of organizations. These networks balance the openness of public blockchains and the control of private blockchains, allowing for collaboration and interoperability while preserving certain levels of privacy and governance (Llamas Covarrubias & Llamas Covarrubias, 2021; Omar & Basir, 2018).

Blockchain technology addresses several limitations of traditional systems in securing digital identities and personal data:

i. Decentralization: By decentralizing trust and eliminating the need for intermediaries, blockchain reduces the risk of single points of failure and enhances resilience against cyberattacks, data breaches, and unauthorized access.

ii. Immutability: The immutable nature of blockchain ensures that once data is recorded on the ledger, it cannot be altered or tampered with without consensus from most network participants. This provides an auditable and transparent record of transactions, enhancing accountability and trust.

iii. Cryptographic Security: Blockchain employs advanced cryptographic techniques, such as hashing and digital signatures, to secure transactions and

protect sensitive information from unauthorized access or manipulation. These cryptographic primitives ensure the confidentiality, integrity, and authenticity of digital identities and personal data stored on the blockchain.

iv. Transparency and Auditability: Public blockchains offer unparalleled transparency, allowing anyone to inspect the ledger and verify transactions in real-time. This transparency fosters trust and accountability, mitigating the risk of fraud, corruption, and data manipulation.

4. APPLICATIONS OF BLOCKCHAIN IN SECURING DIGITAL IDENTITIES AND PERSONAL DATA

Blockchain technology holds immense potential to transform digital identity management and personal data security by offering innovative solutions that prioritize privacy, security, and user control. The following sections explore various use cases and applications of blockchain in this domain:

4.1. Exploration of Various Use Cases and Applications

Blockchain can streamline identity verification processes by providing a secure and tamper-proof ledger of verified identities. For instance, individuals can cryptographically sign their identity documents and store them on the blockchain, enabling instant and verifiable access to their credentials when needed.

Blockchain's immutable nature ensures the integrity of data stored on the ledger, making it suitable for verifying the authenticity and provenance of digital assets and documents. This capability is useful in combating document forgery, counterfeit goods, and fraudulent activities. Blockchain facilitates secure and transparent data sharing among multiple parties without intermediaries. Through encrypted data storage and decentralized access controls, blockchain enables individuals to share sensitive information with trusted entities while maintaining privacy and confidentiality.

4.2. Discussion on How Blockchain Can Enable Self-sovereign Identity

Self-sovereign identity (SSI) refers to individuals having full control and ownership over their digital identities and personal data. Blockchain technology enables SSI by decentralizing identity management and empowering individuals to manage, control, and share their identity attributes without relying on centralized authorities.

Blockchain-based SSI solutions leverage decentralized identifiers (DIDs) and verifiable credentials to enable individuals to create, manage, and selectively disclose their identity attributes. DIDs serve as unique identifiers anchored on the blockchain, while verifiable credentials are cryptographically signed attestations issued by trusted entities. By leveraging SSI principles, individuals can assert their identities across various online services and platforms without repeatedly verifying their identity or sharing sensitive information. This enhances privacy and security and reduces the administrative burden associated with identity management and authentication processes.

4.3. Analysis of Decentralized Authentication and Authorization Mechanisms

Blockchain enables decentralized authentication and authorization mechanisms that eliminate the need for centralized identity providers and intermediaries. Individuals can authenticate themselves and authorize transactions directly on the blockchain network through public-private key cryptography and smart contracts (Hammi, Hammi, Bellot, & Serhrouchni, 2018; Khalid et al., 2020).

Decentralized authentication protocols, such as OpenID Connect and Decentralized Identity Foundation (DIF) standards, enable users to authenticate securely using their blockchain-based digital identities across different services and applications (Kyriakidou, Papathanasiou, & Polyzos, 2023). Smart contracts can enforce fine-grained access control policies, allowing individuals to grant or revoke permissions for accessing their personal data based on predefined rules and conditions. This granular control ensures that only authorized parties can access sensitive information, enhancing privacy and data security (Lux, Thatmann, Zickau, & Beierle, 2020).

Numerous projects and initiatives leverage blockchain technology to enhance identity verification, data encryption, and secure data sharing. For example:

i. Sovrin: Sovrin is a global public utility built on blockchain technology for self-sovereign identity. It enables individuals and organizations to create and manage decentralized identities and verifiable credentials, fostering trust, privacy, and interoperability in the digital ecosystem (Naik & Jenkins, 2021).

ii. Hyperledger Indy: Hyperledger Indy is an open-source project that provides tools and libraries for building decentralized identity systems. It offers a set of interoperable standards and protocols for creating, exchanging, and verifying digital identities and credentials (Chicano Valenzuela, 2022; Dunphy, 2022).

iii. Ocean Protocol: Ocean Protocol is a decentralized data exchange protocol that enables individuals and organizations to publish, access, and monetize data while preserving privacy and data ownership. It leverages blockchain technology to ensure transparent and auditable data transactions (Myadam & Patnam, 2020).

In summary, blockchain technology offers a wide range of applications for securing digital identities and personal data, ranging from identity verification and self-sovereign identity to decentralized authentication and secure data sharing. By prioritizing privacy, security, and user control principles, blockchain empowers individuals to assert ownership over

their digital identities and personal data while fostering trust and transparency in the digital ecosystem.

5. CHALLENGES AND FUTURE DIRECTIONS

Implementing blockchain-based solutions for digital identity and personal data security presents several challenges and limitations that must be addressed. Additionally, exploring potential future developments and advancements in blockchain technology is crucial for overcoming these challenges and realizing its transformative potential in securing digital identities and personal data.

5.1. Examination of Challenges and Limitations

One of the primary challenges facing blockchain technology is scalability. As the number of transactions increases, public blockchain networks may face congestion and slower transaction processing times. This scalability issue hinders the widespread adoption of blockchain-based solutions for digital identity management and personal data security, particularly in high-volume applications.

Blockchain networks often operate in silos, making it challenging to exchange data and assets across different platforms and protocols seamlessly. Interoperability concerns limit the interoperability of blockchain-based identity solutions and hinder their ability to achieve widespread adoption and integration with existing systems. The regulatory landscape surrounding blockchain and digital identity is still evolving, posing challenges for compliance and legal frameworks. Data protection, privacy, and identity verification regulations vary across jurisdictions, creating uncertainty for businesses and organizations implementing blockchain-based solutions for digital identity management and personal data security.

5.2. Future Directions

Future developments in blockchain technology aim to address scalability issues by implementing layer 2 scaling solutions, such as sidechains, state channels, and off-chain scaling protocols. These solutions aim to increase transaction throughput and reduce latency without compromising decentralization or security.

Efforts are underway to develop interoperability standards and protocols that facilitate seamless data exchange and asset transfer across different blockchain networks. Projects such as Cosmos, Polkadot, and interoperability working groups within blockchain consortia aim to bridge the gap between disparate blockchain ecosystems and enable cross-chain communication. As blockchain technology matures, regulatory frameworks are expected to evolve to provide clarity and guidance for businesses and organizations operating in the digital identity space. Collaboration between industry stakeholders, policymakers, and regulators is essential to develop regulatory frameworks that balance innovation with consumer protection and privacy rights.

Future advancements in blockchain technology may focus on enhancing privacy and confidentiality features, such as zero-knowledge proofs, ring signatures, and homomorphic encryption. These privacy-enhancing technologies enable secure and anonymous transactions while preserving the integrity and immutability of the blockchain ledger.

The emergence of decentralized identity ecosystems powered by blockchain technology is expected to reshape the digital identity landscape. These ecosystems enable individuals to own and control their digital identities, fostering trust, privacy, and interoperability across various online platforms and services. Integration of artificial intelligence (AI) and machine learning (ML) algorithms with blockchain technology can enhance identity verification and authentication processes, enabling more efficient and accurate identification of individuals while minimizing the risk of fraud and impersonation.

6. CONCLUSION

In conclusion, blockchain technology holds immense promise in securing digital identities and personal data, offering decentralized, transparent, and tamper-proof solutions. However, several challenges such as scalability issues, interoperability concerns, and regulatory challenges need to be addressed to unlock its full potential.

Future developments in blockchain technology, including scalability solutions, interoperability standards, and privacy-enhancing technologies, are expected to overcome these challenges and drive innovation in digital identity management and personal data security. Collaboration between industry stakeholders, policymakers, and regulators is essential to develop robust regulatory frameworks that promote innovation while safeguarding consumer rights and privacy. Overall, continued research and innovation in blockchain technology are critical for realizing its transformative potential in securing digital identities and personal data, ultimately empowering individuals with greater control over their digital assets and online interactions.

REFERENCES

1. Alston, E., Law, W., Murtazashvili, I., & Weiss, M. (2021). Can permissionless blockchains avoid governance and the law? *Notre Dame J. on Emerging Tech., 2*, 1.
2. Baier, T., Zirpins, C., & Lamersdorf, W. (2003). *Digital identity: How to be someone on the net.* Paper presented at the Proceedings of the IADIS International Conference of e-Society.
3. Beduschi, A. (2019). Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. *Big Data & Society, 6*(2), 2053951719855091.
4. Beduschi, A., Cinnamon, J., Langford, J., Luo, C., & Owen, D. (2017). Building Digital Identities: The Challenges, Risks and Opportunities of Collecting

Behavioural Attributes for new Digital Identity Systems.

5. Bernabe, J. B., Canovas, J. L., Hernandez-Ramos, J. L., Moreno, R. T., & Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: Review and challenges. *IEEE Access*, *7*, 164908-164940.
6. Bietti, E. (2019). Consent as a free pass: Platform power and the limits of the informational turn. *Pace L. Rev.*, *40*, 310.
7. Chicano Valenzuela, D. (2022). *Identifying and tracking physical objects with hyperledger decentralized applications.* Universitat Politècnica de Catalunya,
8. Chua, H. N., Ooi, J. S., & Herbland, A. (2021). The effects of different personal data categories on information privacy concern and disclosure. *Computers & Security*, *110*, 102453.
9. Dunphy, P. (2022). A note on the blockchain trilemma for decentralized identity: Learning from experiments with hyperledger indy. *arXiv preprint arXiv:2204.05784*.
10. Hammi, M. T., Hammi, B., Bellot, P., & Serhrouchni, A. (2018). Bubbles of Trust: A decentralized blockchain-based authentication system for IoT. *Computers & Security*, *78*, 126-142.
11. Huang, D., Chung, C.-J., Dong, Q., Luo, J., & Kang, M. (2019). *Building private blockchains over public blockchains (PoP) an attribute-based access control approach.* Paper presented at the Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing.
12. Jain, R. (2007). Secure Socket Layer (SSL) and Transport Layer Security (TLS). *Washington University, Saint Louis*.
13. Khalid, U., Asim, M., Baker, T., Hung, P. C., Tariq, M. A., & Rafferty, L. (2020). A decentralized lightweight blockchain-based authentication mechanism for IoT systems. *Cluster Computing*, *23*(3), 2067-2087.
14. Knight, A., & Saxby, S. (2014). Identity crisis: Global challenges of identity protection in a networked world. *Computer Law & Security Review*, *30*(6), 617-632.
15. Kyriakidou, C. D. N., Papathanasiou, A. M., & Polyzos, G. C. (2023). Decentralized Identity With Applications to Security and Privacy for the Internet of Things. *Computer Networks and Communications*, 244–271-244–271.
16. Laurent, M., Denouël, J., Levallois-Barth, C., & Waelbroeck, P. (2015). Digital identity. In *Digital identity management* (pp. 1-45): Elsevier.
17. Llamas Covarrubias, J. Z., & Llamas Covarrubias, I. N. (2021). Different types of government and governance in the blockchain. *Journal of Governance and Regulation*, *10*(1).
18. Luevanos, C., Elizarraras, J., Hirschi, K., & Yeh, J.-h. (2017). *Analysis on the security and use of password managers.* Paper presented at the 2017 18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT).
19. Lux, Z. A., Thatmann, D., Zickau, S., & Beierle, F. (2020). *Distributed-ledger-based authentication with decentralized identifiers and verifiable credentials.* Paper presented at the 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS).
20. Mohan, C. (2019). *State of public and private blockchains: Myths and reality.* Paper presented at the Proceedings of the 2019 international conference on management of data.
21. Mueller, M. L., Park, Y., Lee, J., & Kim, T.-Y. (2006). Digital identity: How users value the attributes of online identifiers. *Information Economics and Policy*, *18*(4), 405-422.
22. Myadam, N. G., & Patnam, B. (2020). Design and Implementation of Key Exchange Mechanisms for Software Artifacts using Ocean Protocol. In.
23. Naik, N., & Jenkins, P. (2021). *Sovrin network for decentralized digital identity: Analysing a self-sovereign identity system based on distributed ledger technology.* Paper presented at the 2021 IEEE International Symposium on Systems Engineering (ISSE).
24. Omar, A. S., & Basir, O. (2018). *Identity management in IoT networks using blockchain and smart contracts.* Paper presented at 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).
25. Sullivan, C. (2018). Digital identity–From emergent legal concept to new reality. *Computer Law & Security Review*, *34*(4), 723-731.
26. Suzor, N. P. (2019). *Lawless: The secret rules that govern our digital lives*: Cambridge University Press.
27. Taskinsoy, J. (2019). Blockchain: a misunderstood digital revolution. Things you need to know about blockchain. *Things You Need to Know about Blockchain (October 8, 2019)*.
28. Tene, O., & Polonetsky, J. (2012). Big data for all: Privacy and user control in the age of analytics. *Nw. J. Tech. & Intell. Prop.*, *11*, 239.
29. Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., . . . Moscicki, A. (2017). *Data breaches, phishing, or malware? Understanding the risks of stolen credentials.* Paper presented at the

Proceedings of the 2017 ACM SIGSAC conference on computer and communications security.

30. Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., . . . Kim, D. I. (2019). A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access, 7*, 22328-22370.
31. Windley, P. J. (2005). *Digital Identity: Unmasking identity management architecture (IMA)*: " O'Reilly Media, Inc.".
32. Xu, X., Pautasso, C., Zhu, L., Lu, Q., & Weber, I. (2018). *A pattern collection for blockchain-based applications.* Paper presented at the Proceedings of the 23rd European Conference on Pattern Languages of Programs.
33. Zhu, X., & Badr, Y. (2018). Identity management systems for the internet of things: a survey towards blockchain solutions. *Sensors, 18*(12), 4215.
34. Zwitter, A. J., Gstrein, O. J., & Yap, E. (2020). Digital identity and the blockchain: universal identity management and the concept of the "Self-Sovereign" individual. *Frontiers in Blockchain, 3*, 26.