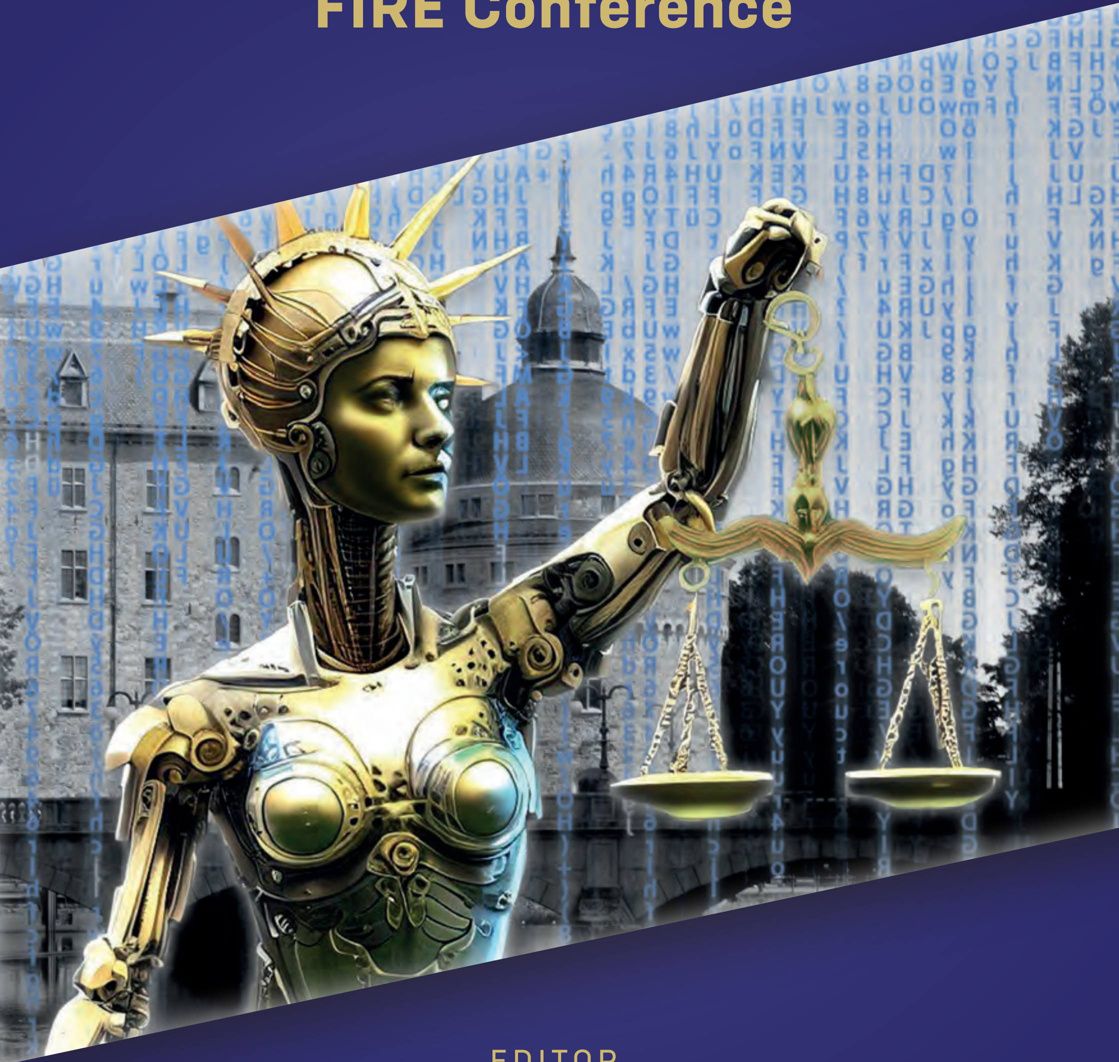
PROCEEDINGS FROM THE FIRST ANNUAL

FIRE Conference



EDITOR

Magnus Kristoffersson

iUSTUS

Proceedings from
the First Annual International

FIRE CONFERENCE

10th–11th of November 2022
Örebro University
Sweden

EDITOR
MAGNUS KRISTOFFERSSON

iUSTUS
FÖRLAG

Table of Contents

Mais Qandeel

Chapter 10 Blockchain Application in Information Ecosystems: The Right to Privacy in Cyberspace

Abstract: This chapter explores whether blockchain technology and its core operational principles – such as decentralisation, transparency, equality and accountability – could play a role in enhancing the protection of human rights in the application of financial information retrieval ecosystems. In this chapter, the legal analysis of such an application focuses on data protection, specifically privacy. Thus, it first discusses how blockchain technology application plays a vital role in realising and challenging data protection. In essence, the chapter seeks to establish how such technological enhancement will securely facilitate governmental and business operations in dealing with data/information from a human rights perspective.

10.1 Introduction

The transformative prospects of distributed ledger technology (DLT) have attracted great interest. Financial institutions are investing heavily in the initial applications of DLT technology. DLT has been used in various applications to enhance efficiency, reduce costs, and ensure immutability, traceability, security, and transparency. In the application of financial retrieval systems, the way data is collected, reported, stored, used, obtained, processed, shared is of utmost importance. Businesses must provide their financial data to the public authorities, depending on the jurisdiction and domestic regulations in place. This data is mostly provided digitally on an annual or monthly basis, which is surrounded by certain complexities and concerns. The existence of an ecosystem that enables businesses and authorities to submit and retrieve data, respectively, provides a digitalized environment with certain probabilities that facilitate the conduct of financial information.

At the same time, this digital ecosystem is encircled with/surrounded by human rights concerns, particularly the protection of individual (data) privacy. Privacy refers to individuals' rights to entirely possess, control and govern the transmission of their own data as to how, when, with whom and how, and for how long.[1] This also concerns the authorization granted to other actors, whether other individuals, public authorities, or corporations. As protected in international, regional and domestic regulations, the right to privacy is one of the main pillars where data is concerned. The question of privacy becomes significant when involving personal and sensitive data. Additionally, the question of the type of technology that is used in such an ecosystem is of great significance. Blockchain technology is today utilized as a harbour of many digital activities, including financial information storage; hence, an attentive assessment of the legal implication of such technology in relation to privacy is needed.

This chapter explores whether blockchain technology and its core operational principles – such as decentralisation, transparency, equality and accountability – could play a role in enhancing the protection of human rights in the application of financial information retrieval ecosystems. In this chapter, the legal analysis of such application focuses on data protection, specifically privacy. Thus, it first discusses how blockchain technology application plays a vital role in realizing and challenging data protection. In essence, the chapter seeks to establish how such technological enhancement will securely facilitate governmental and business operations in dealing with data/information from a human rights perspective.

[1] Singh, A.R. & Gautam, D. R. (2022). Right to Privacy in Cyberspace. In (eds.) Kulshrestha, P., Gautam, R., & Singh, A. Cyber Crime, Regulation and Security: Contemporary Issues and Challenges. The Law Brigade Publisher, 38.

10.2 Features of the Ledgers

This section does not intend to provide a comprehensive and detailed description of distributed ledger technology or fully examine its technical characteristics. It rather sheds light on the main features of ledgers, specifically blockchain technology, and focuses on the portrayal of these features and their connection to privacy issues. The ultimate purpose of this portrayal is to provide an assessment of the challenges and opportunities of blockchain technology when used as a data hub for information ecosystems. To appreciate (data) privacy protection, it is central to look at the current pronounced characteristics of blockchain technology and assess its capabilities.

Distributed ledger technology can hold transactions and interactions to secure communications in a complex information environment, which are at the origin of data creation and collection. In recognition of the importance of accurate and timely information as a precondition for human rights, blockchain technology is a significant framework to increase accountability and transparency for the prevention of human rights abuses. Several questions should be asked: what is distributed ledger technology? What is blockchain technology? What are the distinguishable characteristics of blockchain technology? And what is their connection with privacy? These questions are discussed briefly in this section.

Distributed ledgers are a model of decentralised records where data can be upheld in storage points that are connected. Distributed ledger technology can be defined as "a system for value transactions running on a peer-to-peer (P2P) network that is distributed and does not require a central authority to intermediate those transactions."[2] Blockchain technology is a form of distributed ledger technology, and in the financial world, it can be described as an "accounting book".[3] It is one of the most used and well-known applications for ledgers. Blockchain technology is simply, as the name suggests, a "ledger of transactions, or blocks, that form to make a systematic, linear chain of all transactions ever made.

[2] Li, J., & Kassem, M. (2021) Applications of distributed ledger technology (DLT) and Blockchain-enabled smart contracts in construction. *Automation in Construction 132*(103955), 1–26, 2.

[3] Al-Saqaf, W., & Seidler, N. (2017). Blockchain technology for social impact: opportunities and challenges ahead, *Journal of Cyber Policy, 2*(3), 338–354, 339.

While the blocks themselves are highly encrypted and anonymized, the transaction headers are made public and not owned or mediated by any specific person or entity."[4] Blockchain can be public, alliance/hybrid and private.[5] For the purpose of any intended application of blockchain in a financial information system, it is important to note the permissioned-private blockchain is assumingly the tool to be utilized. Notably, other applications of blockchain technology benefit from being public. Although it was its initial purpose, blockchain technology has moved beyond cryptocurrencies.[6] It has been applied in several application areas[7] such as supply chain management, banking and finance, digital authentication, smart contracts and asset trading. Blockchain technology, in essence, has the potential to transform businesses and their legal and regulatory implications. Remarkably, it could be used in both the public and private sectors.[8] It is, indeed, a potential booster of development and innovation. Blockchain technology has many features, upon which it has gained its popularity. In the process of analysing the legal issues and implication of this technology in relation to privacy, it is vital to identify the main characteristics of blockchain technology.

The main relevant characteristics or features are i) decentralization, ii) cryptography and iii) immutability. First, decentralization is one of the main disguisable characters of blockchain. Instead of relying on a centralized ledger, "many data storage points (nodes) are all connected with each other and store all data simultaneously, together constituting

[4] Hughes, A., Park, A., Kietzmann, J., & Archer-Brown, C. (2019). Beyond Bitcoin: What blockchain and distributed ledger technologies mean for firms, *Business Horizons 62*(3), 273–281, 274.

[5] Chen, Y., Chen, H., Zhang, Y., Han, M., Siddula, M., & Cai, Z. (2022). A Survey on Blockchain Systems: Attacks, Defenses, and Privacy Preservation, *High-Confidence Computing 2*(100048), 1–20, 3.

[6] Zetzsche, D. A., Buckley, R. P., & Arner, D. W. (2018). The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain. *University of Illinois Law Review, 2018*(4), 1361–1406.

[7] Kim, J.W. (2020). Blockchain Technology and Its Applications: Case Studies, *Journal of System and Management Sciences 10*(1), 83–93; See also Casinoa, F., Dasaklisb, T.K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues, *Telematics and Informatics 36*, 55–81.

[8] Hashimy, L., Treiblmaier, H., & Jain, G. (2021). Distributed ledger technology as a catalyst for open innovation adoption among small and medium-sized enterprises, *Journal of High Technology Management Research 32*(100405), 1–10.

the common ledger… [it] requires consensus of those nodes rather than just the confirmation by one hierarchically structured storage device."[9] To put it simply, instead of relying on an intermediary to confirm the data transfer, blockchain requires consensus on such data. This feature creates the potential to increase and foster data security due to the absence of intermediaries.[10]

Second, cryptography refers to the fact that the data stored on blockchain is securely reliant on authorized access. While some blockchains are public, others are private and need a special private key to access. Blockchain maintains "confidentiality of the content and participants in each transaction… [the only one] with the correct key can access the details associated with a specific record."[11] Access to data that is stored on blockchain technology can only be elaborately accessed by an authorized person who holds the 'access key'. From an information security point of view, cryptography can be considered to partially contribute to the fulfilment of the C.I.A. information security triangle, namely, confidentiality, integrity and availability of information.[12] The designed cryptographic nature of the blockchain increases cybersecurity and could be sufficient to resist hacking and security threats.[13] Cryptography is vital to ensure that the transferred and stored data is secure, which is coupled with the idea of privacy.

Third, immutability means, in simple terms, that all data and transactions that exist on blockchain cannot be edited, reversed, altered or

[9] Zetzsche, D. A., Buckley, R. P., & Arner, D. W. (2018). The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain. *University of Illinois Law Review, 2018*(4), 1361–1406, 1371.

[10] Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering, 59*(3), 183–187, 184.

[11] McLean, S., & Deane-Johns, S. (2016) Demystifying Blockchain and Distributed Ledger Technology – Hype or Hero? *Computer Law Review International, 17*(4), 97–102, 97.

[12] Bosworth, S., Kabay, M.E., & Whyne, E. (eds.) (2014) Computer Security Handbook, (6th ed.). Wiley; See also Samonas, S., & Coss, D. (2014). The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security, *Journal of Information System Security 1*(3), 21–45.

[13] Hasanova, H., Baek, U., Shin, M., Cho, K., & Kim, M.-S. (2019). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *International Journal of Network Management, 29* (e2060), 1.

deleted. It "refers to the fact that no participant in a blockchain initiative can tamper with a transaction once it is agreed upon."[14] This unique characteristic of blockchain technology makes it extremely transparent[15] and ensures authenticity, where the manipulation and corruption of data cannot be inflicted. This is what can be identified here as *transparency by design*. Immutability scores high in blockchain technology design, hence the name *immutability by design*. At the same time, this very same characteristic has raised concerns regarding errors that have occurred and enforceability issues. At the European level, for instance, this immutability characteristic explicitly opposes compliance with the erasing requirements imposed by the General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), particularly the right to erasure / be forgotten.[16]

Although these characteristics of blockchain technology are surrounded by claims of increasing cybersecurity,[17] some studies on the security and privacy of blockchain technology have shown that "many applications [of blockchain] have fallen victim to successful cyberattacks."[18] There are several challenges concerning and notable attacks on blockchain applications that have occurred in the last few years.[19] For example, the hacking of Mt.Gox, a Bitcoin exchange resulting in 473 million US dollars' worth of losses, and Ether currency where USD 53 million were wrongly channelled to a third party, and in some of the attacks "[t]he White Hat Group breached the wallets using the same vulnerability as the attackers and funneled the funds into the group's

[14] Malhotra, A., O'Neill, H., & Stowell, P. (2022). Thinking strategically about blockchain adoption and risk mitigation, *Business Horizons 65*, 159–171, 160.

[15] Mohanta, B.K., Jena, D., Panda, S.S., & Sobhanayak, S. (2019) Blockchain Technology: A Survey on Applications and Security Privacy Challenges, *Internet of Things 8*(100107).

[16] Politou, E., Casino, F., Alepis, E. & Patsakis, C. (2021) Blockchain Mutability: Challenges and Proposed Solutions, in IEEE Transactions on Emerging Topics in Computing, 9(4), 1972–1986.

[17] Mathew, A. R. (2019) Cyber Security through Blockchain Technology, *International Journal of Engineering and Advanced Technology 9*(1), 3821–3824.

[18] Hasanova, H., Baek, U., Shin, M., Cho, K., & Kim, M.-S. (2019). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. *International Journal of Network Management, 29* (e2060), 1.

[19] Deshpande, A., Stewart, K., Lepetit, L., & Gunashekar, S. (2017). Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards, (UK: British Standards Institution).

own account."[20] In 2022, Binance, the world's biggest cryptocurrency exchange, suffered a hack, targeting vulnerabilities in its blockchain that serves the assets transfers between networks, with loses estimated at USD 570 million.[21] Such attacks are only examples of the vulnerabilities that surround blockchain application. Simply put, blockchain technology, despite all the promising features, can be and has been subject to cyber-attacks. Blockchain's vulnerabilities are predominantly coupled with privacy concerns. The attacks targeted against blockchain applications genuinely raise concerns in connection with network communications as "privacy leakage is gradually increasing."[22] In response to privacy concerns, some data brokers (database providers) have attempted to minimize sensitive identifiable information.[23] Attacks that lead to, among others, communication interferences, damage or corrupt data, and access to confidential and sensitive data, including biometric and metadata, can result in breaches to the protected right to privacy.

10.3 The Right to Privacy in Cyberspace

The right to privacy in cyberspace has attracted enormous attention at all levels – national, regional and international. Such attention is present in the application of technologies in all fields, whether in law, judiciary, finance, informatics, governance and public sectors, among others. Concerns about the right to privacy, in particular, data privacy have been continuedly raised. In the application of blockchain technology in financial information systems, concerns about data privacy cannot be

[20] Zetzsche, D. A., Buckley, R. P., & Arner, D. W. (2018). The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain. *University of Illinois Law Review, 2018*(4), 1361–1406, 1367–1369.

[21] Livni, E. (7 October 2022). Binance Blockchain Hit by $570 Million Hack, Exposing Crypto Vulnerabilities, *New York Times* https://www.nytimes.com/2022/10/07/business/binance-hack.html accessed 24 January 2023.

[22] Chen, Y., Chen, H., Zhang, Y., Han, M., Siddula, M., & Cai, Z. (2022). A Survey on Blockchain Systems: Attacks, Defenses, and Privacy Preservation, High-Confidence Computing 2:100048, 1–20, 1.

[23] Gindin, S. E. (1997). Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet. *San Diego Law Review, 34*(3), 1153–1224, 1160; see also Kang, J., (1998). *Information Privacy in Cyberspace Transactions, Stanford Law Review, 50*(4), 1193–1294.

ignored. In order to ensure the privacy requirements of the data when transferred, retrieved, processed, used, stored, shared and obtained, the nexus between data privacy and blockchain must be understood. This is the purpose of this section.

The protection of human rights generally applies offline and online.[24] Privacy[25] (of data) in the cyberspace has gained special attention, and it is described as "central to the enjoyment… of human rights online… [and] one of the foundations of a democratic society…"[26] The Charter of Human Rights and Principles for the Internet includes data privacy as one of its main pillars. Principle 5: Privacy and Data Protection precisely provides that:

> Everyone has the right to privacy online. This includes freedom from surveillance, the right to use encryption, and the right to online anonymity. Everyone also has the right to data protection, including control over personal data collection, retention, processing, disposal and disclosure.[27]

At the regional and domestic levels, (data) privacy is also well-protected. For example, the European General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR), the Swedish Data Protection Act (2018:218) and California Consumer Privacy Act of 2018 (CCPA) give individuals i) more power and control over their own personal data that governments and businesses collect and possess about them and ii) more privacy protection with very peculiar securities such as the right to know,

[24] Human Rights Council Res. 20/8 (2012). The promotion, protection and enjoyment of human rights on the Internet, UN Doc. No. A/HRC/RES/20/8 (16 July 2012).

[25] The right to privacy is internationally protected in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights, which both provide that: 1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2) Everyone has the right to the protection of the law against such interference or attacks.

[26] United Nations Human Rights Office of the High Commissioner (2021). International Standards: OHCHR and Privacy in the Digital Age, https://www.ohchr.org/en/privacy-in-the-digital-age/international-standards accessed 25 January 2023.

[27] United Nations Internet Governance Forum (2014). The Charter of Human Rights and Principles for the Internet (August 2014 – 4th Edition) https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf accessed 25 January 2023.

the right to consent, the right to delete/oblivion, the right to opt-out, the right to correct and the right to limit. Blockchain is seen as a challenge to these legal requirements, specific to their contexts and jurisdictions.

The protection of data privacy is well-established. International law, [s]tatutory, common law, and constitutional privacy rights rest on diverse assumptions about the nature and purposes of privacy"[28] Individuals have the right to control all aspects of their data, as to where it is stored, how, why, and by whom it is used, for what purposes and for how long it is being handled. Derived from its vital significance, privacy has been comprehensively discussed by the United Nations General Assembly (UN GA), Human Rights Council (HRC) and legal scholars nationally and internationally. In its resolution 75/176 of 2020, the UN GA highlighted the obligations of public authorities and business enterprises concerning data privacy. For the interest of this chapter, the subject matters to emphasize are the relationship between public authorities and business enterprises in connection with handling data. The resolution provides that States must take "measures to prevent the unlawful retention, processing and use of personal data stored by public authorities and business enterprises",[29] where there must be "transparency measures with regard to requests by State authorities for access to private user data and information."[30]

In order to protect data privacy, the use of secure and safe technological applications, the choice of what technology to apply becomes central. For this specific need, arguably, blockchain technology can preliminarily offer a promising secure venue for informational ecosystems. This ultimate goal is reflected in the HRC, where it is of utmost importance that public authorities and business enterprises use "technical solutions to secure and to protect the confidentiality of digital communications, including

[28] Byford, K. (1998). Privacy in Cyberspace: Constructing a Model of Privacy for the Electronic Communications Environment. *Rutgers Computer & Technology Law Journal, 24*(1), 1–74.

[29] United Nations General Assembly Resolution 75/176 (2020). The right to privacy in the digital age, UN Doc. No. A/RES/75/176 A/RES/75/176 (16 December 2020), 3.

[30] United Nations General Assembly Resolution 75/176 (2020). The right to privacy in the digital age, UN Doc. No. A/RES/75/176 A/RES/75/176 (16 December 2020), 7.

measures for encryption, pseudonymization and anonymity."[31] The use of proper technical solutions would, in principle, provide for privacy risk management and governance mechanisms, which is recommended by the UN Special Rapporteur on the right to privacy.[32] This, however, needs to be approached with caution. Technical solutions may be inspired by, for instance, privacy by design and data protection.[33]

Studies have shown that the use of blockchain applications is combined with considerable risks to privacy.[34] In other words, "even when users are hiding behind multiple pseudonyms, these can be correlated and often identify them… the fact that transactions are linked, one can retrieve the full history of all transactions performed on a blockchain. "[35] This entails that privacy cannot be achieved simply because privacy was never the purpose of blockchain. In order to make blockchain privacy sensitive, it can be combined with other technologies that offer privacy by design where data is conducted to provide authenticity guarantees. For that purpose, it is noteworthy to indicate that, as Ethereum Foundation puts it, "blockchains do NOT solve privacy issues, and are an authenticity solution only… putting [any data] records in plaintext onto a blockchain is a Very Bad Idea."[36] As long as the data is stored in an encrypted format, where it cannot be tampered with or deleted, blockchain can

[31] United Nations Human Rights Council Res. 42/15 (2019). The right to privacy in the digital age, UN Doc. No. A/HRC/RES/42/15 (7 October 2019), 3.

[32] United Nations Special Rapporteur on the right to privacy (2020). Report pursuant to Human Rights Council resolution 28/16, UN Doc. No. A/HRC/43/52 (24 March 2020) 20.

[33] Rachovitsa, A. (2016) Engineering and lawyering privacy by design: Understanding online privacy both as a technical and an international human rights issue. *International Journal of Law and Information Technology 24*, 374.

[34] Meiklejohn, S. (2018). Top Ten Obstacles along Distributed Ledgers' Path to Adoption, *IEEE Security Privacy*, *16*(4), 13–19; Meiklejohn S., et al. (2013). A Fistful of Bitcoins: Characterizing Payments Among Men with No Names, in Proc. Conf. Internet Meas. Conf., 127–140; Goldfeder, S., Kalodner, H., Reisman, D., & Narayanan, A., (2018). When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies, Proc. Privacy Enhancing Technol., 2018(4), 179–199.

[35] Politou, E., Casino, F., Alepis, E., & Patsakis, C. (2021). Blockchain Mutability: Challenges and Proposed Solutions, *IEEE Transitions 9*(4), 1972–1986, 1976.

[36] Buterin V. (15 January 2016). Privacy on the Blockchain, *Ethereum Foundation Blog*, https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/ accessed 25 January 2023.

moderately satisfy privacy requirements. This, conversely, created other sets of problems, as the data cannot be removed, and long-term data protection becomes a challenge.[37]

The submission of such a requirement comes in handy when thinking of blockchain technology and its defined characteristics, explicitly encryption, on the one hand. On the other, the much-desired characteristic in some practices becomes a disadvantage for others. When using blockchain technology in information ecosystems, transparency may become a downside, where all information is exposed unwittingly and unnecessarily. The current state-of-the-art shows that blockchain still raises problems as regards, enter alia, privacy issues, namely: pseudo-anonymity, immutability, where failure to meet privacy requirements as such, responsibility, accountability[38] and States' obligations[39] become an integral part of the legal discussion of blockchain technology. Eventually, questions concerning law compliance are essential to bridge the gap between law and technology. Whether the law should adopt to technological advancements and features or vice versa is the focus of the next section.

10.4 Law Compliance or Technology Compliance

The disconnect between law and technology can make it difficult to reconcile current data protection laws with the core characteristics of blockchain, such as the lack of centralization, immutability and perpetual data storage. The current state of affairs of regulatory guidance limits opportunities for an effective reconciliation between law provisions and blockchain technology. It is crucial then to think of the law as a flexible protection instrument or reverse that thinking if indispensable. If the law

[37] Beduschi, A. (2019). Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. *Big Data & Society 6*(2), 1–6, 2.

[38] Busstra, M. (2020). Designing for Good: Blockchain Technology and Human Rights. *Intergovernmental Organisations In-house Counsel Journal 2020*, 31–38.

[39] Hughes, K. (2017). Blockchain, The Greater Good, and Human and Civil Rights. *Metaphilosophy 48*(5), 654–665.

is deemed hard and inflexible, would the technology have to adopt its features to be law compliant – here technology developers and computer scientists are concerned. This is a remarkable intersection between law and technology.

When computer scientists ensure that technology by-design meets the existing regulatory framework, this creates a type of technology that is law compliant,[40] this is what I call *law compliant technology*. In this case, lawmakers and judiciary, within the existing legal framework, develop the legal norms and their application. This would not require any ground-breaking rules or be confronted with unforeseeable violations. In the real and digital worlds, this is not the case. Technology has proved that it has no boundaries and comes to challenge the law, not to obey it. Possible legal capacity for extending the scope of existing legal provisions to encompass new activities that should/should not be covered by the law (domestic, regional or international) is questionable. Thus, can the laws and regulations demand that properties of blockchain technology should be changed? This is very unlikely. Regulators tend to put limitations on the use of technologies and address their implications.

Consequently, this limits the discussion to the ability of the law to follow-up technological developments. This is what I identify as *technology compliance* with limitations. There are two scenarios here to point out: the first scenario concerns whether the law should rapidly be made up to date considering the development and implications of technologies, and the second scenario concerns whether the law should restrict the application of technologies for mitigating risks and preventing violations. The answers to these two scenarios are short. It has been established that blockchains have regulatory issues.[41] As technology develops, the law must adapt rapidly.[42] Simply put, the regulatory framework must be able to address the regulatory and human rights issues, namely privacy, pertaining from the use and implementation of blockchain technologies.

[40] Packin, N. (2018). Regtech, Compliance and Technology Judgement Rule. *Chicago-Kent Law Review, 93*(1), 193–220.

[41] Yeoh, P. (2017). Regulatory issues in blockchain technology. *Journal of Financial Regulation and Compliance, 25*(2) 196–208.

[42] Finck, M. (2019). Blockchains: Regulating the Unknown. *German Law Journal 19*(4), 665–692.

The best way, or perhaps the only way, to ensure that blockchain is privacy compliant is to limit its use, depending on the purpose and the sought after benefits. Blockchain enhances transparency but has vulnerabilities. This can be done through legal design and stronger implementation to provide for legal protection mechanisms for privacy-preserving blockchain application. The lawmakers first need to fully understand the technology itself, then design, in consultation with blockchain developers, regulations that fit best. Blockchain governance in the public sector[43] has already been suggested. However, laws must mostly address the legal implications pertaining to the use of blockchain, particularly when sensitive and personal data is involved.

10.5 Conclusions

Financial information continuously involves individual and sensitive data. The use of blockchain technology raises legal issues and privacy concerns. Today, the lack of unambiguous regulations to curb the use of the various types of technologies forces an assessment of the very basic legal principles and existing norms. It might be very unrealistic to expect that the law should step in and address every single application of technology and then foresee its use and misuse. The law should be general in order to accommodate an expansive range of technological applications. Then an assessment of the use of these technologies and their peculiarities becomes a need.

For the very purpose of privacy, the application of blockchain technology as a hub for storing, maintaining, obtaining, sharing, rederiving and using data in a financial information system might not be the best option. However, blockchain technology is a distinct tool if used in combination with other technologies that preserve (data) privacy. This is to ensure that a combination of the most important features that technologies can offer eliminates law non-compliance and provides the best solutions. Changning the human rights approach or making exceptions for each

[43] Tan, E., Mahula, S., & Crompvoets, J. (2022). Blockchain governance in the public sector: A conceptual framework for public management. *Government Information Quarterly 39*(101625), 1–11.

technology is not a viable legal option. Changing blockchain properties and characteristics does not seem achievable. A new technology that combines the best of all technologies could be the new way. This would possibly bridge the gap between law and technology and would reconcile current data protection laws with the core characteristics of blockchain in the use of financial information systems.

References

Al-Saqaf, W., & Seidler, N. (2017). Blockchain Technology for Social Impact: Opportunities and Challenges Ahead, *Journal of Cyber Policy, 2*(3), 338–354.

Beduschi, A. (2019). Digital Identity: Contemporary Challenges for Data Protection, Privacy and Non-discrimination Rights. *Big Data & Society, 6*(2), 1–6.

Bosworth, S. Kabay, M.E., & Whyne, E. (eds.) (2014). Computer Security Handbook (6th ed.). Wiley.

Busstra, M. (2020). Designing for Good: Blockchain Technology and Human Rights. *Intergovernmental Organisations In-house Counsel Journal 2020*, 31–38.

Buterin V. (15 January 2016). Privacy on the Blockchain, Ethereum Foundation Blog, https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/.

Byford, K. (1998). Privacy in Cyberspace: Constructing Model of Privacy for the Electronic Communications Environment. *Rutgers Computer & Technology Law Journal, 24*(1), 1–74.

Casinoa, F., Dasaklisb, T.K., & Patsakis, C. (2019). A Systematic Literature Review of Blockchain-based Applications: Current Status, Classification and Open Issues. *Telematics and Informatics, 36*, 55–81.

Chen, Y., Chen, H., Zhang, Y., Han, M., Siddula, M., & Cai, Z. (2022). A Survey on Blockchain Systems: Attacks, Defenses, and Privacy Preservation. *High-Confidence Computing, 2*:100048, 1–20.

Deshpande, A., Stewart, K., Lepetit, L., & Gunashekar, S. (2017). Distributed Ledger Technologies/Blockchain: Challenges, Opportunities and the Prospects for Standards (UK: British Standards Institution).

Finck, M. (2019). Blockchains: Regulating the Unknown. *German Law Journal, 19*(4), 665–692.

Gindin, S. E. (1997). Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet. *San Diego Law Review, 34*(3), 1153–1224.

Goldfeder, S., Kalodner, H., Reisman, D., & Narayanan, A. (2018). When the Cookie Meets the Blockchain: Privacy Risks of Web Payments via Cryptocurrencies, Proc. *Privacy Enhancing Technol., 2018*(4), 179–199.

Hasanova, H., Baek, U., Shin, M., Cho, K., & Kim, M-S. (2019). A Survey on Blockchain Cybersecurity Vulnerabilities and Possible Countermeasures. *International Journal of Network Management, 29* (e2060), 1.

Hashimy, L., Treiblmaier, H., & Jain, G. (2021). Distributed Ledger Technology as a Catalyst for Open Innovation Adoption Among Small and Medium-sized Enterprises. *Journal of High Technology Management Research, 32*(100405), 1–10.

Hughes, A., Park, A., Kietzmann, J., & Archer-Brown, C. (2019). Beyond Bitcoin: What Blockchain and Distributed Ledger Technologies Mean for Firms. *Business Horizons 62*(3), 273–281.

Hughes, K. (2017). Blockchain, The Greater Good, and Human and Civil Rights. *Metaphilosophy, 48*(5), 654–665.

Kang, J. (1998). Information Privacy in Cyberspace Transactions. *Stanford Law Review, 50*(4), 1193–1294.

Kim, J.W. (2020). Blockchain Technology and Its Applications: Case Studies. *Journal of System and Management Sciences, 10*(1), 83–93.

Li, J., & Kassem, M. (2021). Applications of Distributed Ledger Technology (DLT) and Blockchain-enabled Smart Contracts in Construction. *Automation in Construction, 132*(103955), 1–26.

Livni, E. (7 October 2022). Binance Blockchain Hit by $570 Million Hack, Exposing Crypto Vulnerabilities, *New York Times* https://www.nytimes.com/2022/10/07/business/binance-hack.html.

Malhotra, A., O'Neill, H., & Stowell, P. (2022). Thinking Strategically about Blockchain Adoption and Risk Mitigation. *Business Horizons, 65*, 159–171.

Mathew, A. R. (2019). Cyber Security through Blockchain Technology, *International Journal of Engineering and Advanced Technology, 9*(1), 3821–3824.

McLean, S., & Deane-Johns, S. (2016). Demystifying Blockchain and Distributed Ledger Technology – Hype or Hero?. *Computer Law Review International, 17*(4), 97–102.

Meiklejohn S., et al. (2013). A Fistful of Bitcoins: Characterizing Payments Among Men With no Names, in Proc. Conf. Internet Meas. Conf., 127–140.

Meiklejohn, S. (2018). Top Ten Obstacles Along Distributed Ledgers Path to Adoption. *IEEE Security Privacy, 16*(4), 13–19.

Mohanta, B.K., Jena, D., Panda, S.S., & Sobhanayak, S. (2019). Blockchain Technology: A Survey on Applications and Security Privacy Challenges. *Internet of Things, 8*(100107).

Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). Blockchain. *Business & Information Systems Engineering, 59*(3),183–187.

Packin, N. (2018). Regtech, Compliance and Technology Judgment Rule. *Chicago-Kent Law Review, 93*(1), 193–220.

Politou, E., Casino, F., Alepis, E. & Patsakis, C. (2021). Blockchain Mutability: Challenges and Proposed Solutions, in *IEEE Transactions on Emerging Topics in Computing, 9*(4), 1972–1986.

Rachovitsa, A. (2016). Engineering and Lawyering Privacy by Design: Understanding Online Privacy both as a Technical and an International Human Rights Issue. *International Journal of Law and Information Technology, 24*, 374.

Samonas, S., & Coss, D. (2014). The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security. *Journal of Information System Security, 1*(3), 21–45.

Singh, A.R. & Gautam, D. R. (2022). Right to Privacy in Cyberspace. In (eds.) Kulshrestha, P., Gautam, R., & Singh, A. Cyber Crime, Regulation and Security: Contemporary Issues and Challenges. The Law Brigade Publisher.

Tan, E., Mahula, S. & Crompvoets, J. (2022). Blockchain Governance in the Public Sector: A Conceptual Framework for Public Management. *Government Information Quarterly, 39*(101625) 1–11.

United Nations General Assembly Resolution 75/176 (2020). The Right to Privacy in the Digital Age, UN Doc. No. A/RES/75/176 A/RES/75/176 (16 December 2020).

United Nations Human Rights Council Res. 20/8 (2012). The Promotion, Protection and Enjoyment of Human Rights on the Internet, UN Doc. No. A/HRC/RES/20/8 (16 July 2012).

United Nations Human Rights Council Res. 42/15 (2019). The Right to Privacy in the Digital Age, UN Doc. No. A/HRC/RES/42/15 (7 October 2019), 3.

United Nations Human Rights Office of the High Commissioner (2021). International Standards: OHCHR and Privacy in the Digital Age, https://www.ohchr.org/en/privacy-in-the-digital-age/international-standards accessed 25 January 2023.

United Nations Internet Governance Forum (2014). The Charter of Human Rights and Principles for the Internet (August 2014 – 4th Edition) https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/Communications/InternetPrinciplesAndRightsCoalition.pdf accessed 25 January 2023.

United Nations Special Rapporteur on the Right to Privacy (2020). Report pursuant to Human Rights Council resolution 28/16, UN Doc. No. A/HRC/43/52 (24 March 2020) 20.

Yeoh, P. (2017). Regulatory Issues in Blockchain Technology. *Journal of Financial Regulation and Compliance, 25*(2) 196–208.

Zetzsche, D. A., Buckley, R. P., & Arner, D. W. (2018). The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain. *University of Illinois Law Review, 2018*(4), 1361–1406.