THIS ANTHOLOGY IS A COLLECTION of scholarly articles drawn from contributions to the inaugural international and interdisciplinary conference of the Financial Information Retrieval Ecosystem (FIRE) research project. This conference took place from November 10th to 11th in 2022 at Örebro University, Sweden, and was generously financed by the Riksbankens Jubileumsfond.

The FIRE consortium is an international and interdisciplinary research collective unified by a core inquiry: how is society, particularly from a legal viewpoint, being fundamentally reshaped by the swift digitalisation of business-related information? This inquiry deeply resonates at both national and international echelons, given the extensive influence digitalisation holds over the social, economic, and legal dimensions of our global society. Furthermore, the commitment of Örebro University extends beyond hosting the conference. They have generously funded the open access publication of this anthology.
Proceedings from
the First Annual International
FIRE
CONFERENCE
10th–11th of November 2022
Örebro University
Sweden
EDITOR
MAGNUS KRISTOFFERSSON
# Table of Contents

Preface 7

The Authors 11

*Magnus Kristoffersson*
Chapter 1
An Overview of the FIRE Research Project 15

*Rigmor Argren*
Chapter 2
Using the European Convention on Human Rights to Shield Citizens from Harmful Datafication 43

*Giovanni Botto*
Chapter 3
Blockchain and European Administrative Integration: a Reflection on Public Governance and Technology, Starting from the European Competition Field 61

*Clémence Garcia and Takeo Itabashi*
Chapter 4
An Experiment on Double Entry Bookkeeping and Financial Reporting Using Blockchain 75

*Hanna Grylin*
Chapter 5
Income taxation of forestry, forest deduction and digitalization 93

*David Hadwick*
Chapter 6
Breaking the Fiscal Omerta: The Roadmap to Transparency in EU Tax Algorithmic Governance 107
Table of Contents

Jan Kellgren
Chapter 7
The Current Corporate Income Tax Rule Architecture & Automated, Real-Time Taxation – Would the Necessary Prerequisites of Today’s Tax Rules Have to Be Changed? 127

Eleonor Kristoffersson
Chapter 8
ViDA – VAT in the Digital Age 143

Yurii Orzikh
Chapter 9
Accounting Regulation and Financial Reporting under Ukrainian Legislation 153

Mais Qandeel
Chapter 10
Blockchain Application in Information Ecosystems: The Right to Privacy in Cyberspace 177

Francesco Paolo Schiavone
Chapter 11
The Free Movement of Capital within The EU and Digitalisation: The Role of Cryptocurrencies 193

Vadym Tsymbal
Chapter 12
The Digitalization of Governance and Tax Administration in Ukraine 209

Sam van der Vlugt
Chapter 13
Ensuring an Inclusive Shift Towards a Technology-Driven Dialogue Between Taxpayer and Administration: How the Law Can Benefit from a Different Methodology 229

Anna Husman
Chapter 14
Automation in the Public Sector and the Principle of Non-Discrimination 249
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. 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.

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." Blockchain technology is a form of distributed ledger technology, and in the financial world, it can be described as an "accounting book". 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.

---


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."\textsuperscript{4} Blockchain can be public, alliance/hybrid and private.\textsuperscript{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.\textsuperscript{6} It has been applied in several application areas\textsuperscript{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.\textsuperscript{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


the common ledger… [it] requires consensus of those nodes rather than just the confirmation by one hierarchically structured storage device.”

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.

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.” 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. The designed cryptographic nature of the blockchain increases cybersecurity and could be sufficient to resist hacking and security threats. 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

deleted. It “refers to the fact that no participant in a blockchain initiative can tamper with a transaction once it is agreed upon.”\textsuperscript{14} This unique characteristic of blockchain technology makes it extremely transparent\textsuperscript{15} and ensures authenticity, where the manipulation and corruption of data cannot be inflicted. This is what can be identified here as \textit{transparency by design}. Immutability scores high in blockchain technology design, hence the name \textit{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.\textsuperscript{16}

Although these characteristics of blockchain technology are surrounded by claims of increasing cybersecurity,\textsuperscript{17} some studies on the security and privacy of blockchain technology have shown that “many applications [of blockchain] have fallen victim to successful cyberattacks.”\textsuperscript{18} There are several challenges concerning and notable attacks on blockchain applications that have occurred in the last few years.\textsuperscript{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

own account.” 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. 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.” In response to privacy concerns, some data brokers (database providers) have attempted to minimize sensitive identifiable information. 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

---


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.\(^\text{24}\) Privacy\(^\text{25}\) (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…”\(^\text{26}\) 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.\(^\text{27}\)

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,

---


\(^{25}\) 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.


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, statutory, common law, and constitutional privacy rights rest on diverse assumptions about the nature and purposes of privacy. 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”, where there must be “transparency measures with regard to requests by State authorities for access to private user data and information.”

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

---

measures for encryption, pseudonymization and anonymity.”\textsuperscript{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.\textsuperscript{32} This, however, needs to be approached with caution. Technical solutions may be inspired by, for instance, privacy by design and data protection.\textsuperscript{33}

Studies have shown that the use of blockchain applications is combined with considerable risks to privacy.\textsuperscript{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.”\textsuperscript{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.”\textsuperscript{36} As long as the data is stored in an encrypted format, where it cannot be tampered with or deleted, blockchain can

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

---


187
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,\textsuperscript{40} this is what I call \textit{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 \textit{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.\textsuperscript{41} As technology develops, the law must adapt rapidly.\textsuperscript{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.

Chapter 10 Blockchain Application in Information Ecosystems: The Right …

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\textsuperscript{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. Changing the human rights approach or making exceptions for each

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


Mais Qandeel


