International Journal of Law in Context (2023), **19**, 51–69
doi:10.1017/S1744552322000465

§

SPECIAL ISSUE ARTICLE

Layers of privacy in the blockchain: from technological solutionism to human-centred privacy-compliance technologies

Pablo Marcello Baquero*

Assistant Professor, HEC Paris, France
*Corresponding author. E-mail: baquero@hec.fr

Abstract
Different organisations recently published reports identifying the challenges and potential solutions to ensure privacy in blockchain platforms. The proposed solutions frequently emphasise the role of privacy-compliance technologies to be incorporated into the blockchain design. Often, these solutions imply a techno-regulatory approach, ignoring that the level of privacy implemented in a blockchain involves legal and policy choices, disregarding the need to implement human participation and contestability in these platforms. Against this backdrop, this paper proposes to examine how privacy-compliance technologies can incorporate human participation and contestability: first, resorting to the interdisciplinary literature to examine how technological design could balance privacy with human oversight; second, discussing the challenges to ensure *ex post* contestability for aggrieved data subjects; third, examining the difficulties in identifying liable parties in a blockchain platform. The current disregard of the social and human element risks undermining the role of privacy-compliance technologies in the blockchain.

Keywords: blockchain; data protection; privacy compliance technologies; human-centred technologies

1 Introduction

As blockchain projects increasingly emerge across different business sectors (Zhao *et al.*, 2016), so are rising the concerns about data protection in decentralised ledger platforms (Casino *et al.*, 2019, p. 66). Recently, the EU (European Parliament, 2019; European Union Blockchain Observatory Forum, 2018), the French National Data Protection Authority (Daoui *et al.*, 2019) and the Law Society of England and Wales (2020) published reports identifying the challenges and potential solutions to ensure privacy in blockchain platforms. In essence, the challenges relate to the difficulties of applying data protection principles that were conceived for the context of centralised platforms in the Internet (the 'platform economy'), which can be clearly deemed responsible for controlling and processing data, to the blockchain context of distributed, 'immutable' platforms, where the possibilities to modify data are more limited and control over data is diffused – or at least more difficult to be identified (De Filippi, 2016; Finck, 2018a, p. 89). These difficulties are particularly relevant in permissionless blockchain platforms – the focus of this paper – where there is no centralised entity determining a priori who can add new content to the blockchain (as opposed to permission-based blockchain; see Teperdjian, 2019, p. 283).

The solutions proposed often involve privacy-compliance technologies to be incorporated into the design of blockchain platforms to promote compliance with the General Data Protection Regulation (GDPR) legal principles (European Parliament, 2019, pp. 28ff.; Law Society of England and Wales, 2020, pp. 69ff.). Furthermore, these solutions often imply a techno-regulatory approach (Leenes, 2011), idealising the ability of these technologies to evolve to a state-of-the-art where they will be able to automatically solve difficulties concerning privacy in the blockchain, ignoring that they can

be designed in different ways, with different legal and policy implications, and disregarding the need to incorporate human participation and contestability into their design.

This paper, in contrast, claims that the design and mode of implementation of these technologies may occur in different ways, with several limitations, and potentially with highly disparate legal and policy implications. To what extent should anonymity be allowed in the blockchain? Who should be able to contest the design and implementation of data protection in the blockchain? These decisions, which are often bypassed by legal studies and left in the hands of the engineers designing the technology, may be decisive in determining whether and to what extent data protection in the blockchain can prevail.

This issue is examined by looking at how privacy-compliance technologies and the legal framework surrounding them should be designed to facilitate human participation and contestability in the development and implementation of these tools. For that purpose, it focuses on three crucial aspects. First is the need to design blockchain platforms/applications that combine a certain level of human oversight with privacy aspects. Second is the need to allow effective *ex post* contestability regarding privacy design and data protection violations in the blockchain. Third is by analysing the issue of who should be liable for data protection violations in the blockchain. These different aspects, often neglected in the relevant literature, will be crucial to determine whether data protection can be truly implemented in the blockchain.

The paper seeks to fill a gap in the literature that either adopts a techno-regulatory approach regarding privacy-compliance technologies in the blockchain or simply does not deepen the discussions concerning the connection between the human and technological element. For, indeed, the human element in the blockchain has been 'under-theorized and underutilized' (Fairfield, 2019).

In contrast, an emerging literature highlights that blockchain technologies create an 'architecture of trust' (Werbach, 2018) or represent a 'confidence machine' (De Filippi *et al.*, 2020). Instead of dispensing with a human element such as trust, the structure of blockchain converts the traditional forms of trust into different patterns (see section 4).

The remainder of the paper is divided into four parts. In the second part, it reviews the literature on the vulnerabilities of data in the blockchain and challenges for implementing the GDPR. Third, it examines the different privacy-compliance technologies and privacy coins that are being designed to fulfil these objectives. The fourth part discusses how to promote social, trust or human-centred privacy-compliance technologies: first, by resorting to the interdisciplinary literature and to a technical project involving a privacy coin to examine how technological design could combine privacy with a certain level of human oversight; second, by examining how *ex post* contestability could be ensured for data subjects aggrieved by data protection violations; third, by examining challenges to identify liable parties in a blockchain platform. Section 5 concludes.

2 Data protection in the public blockchain: data vulnerabilities and challenges for GDPR implementation

After distinguishing between public, private and consortium blockchain (section 2.1), this section analyzes the main vulnerabilities of data stored in the blockchain (section 2.2) and the challenges of implementing the data protection principles enshrined in the GDPR in such a context (section 2.3).

2.1 The emphasis on public blockchain vs. private or consortium blockchain: different challenges

In discussing the challenges of data protection in the blockchain, it is crucial to distinguish between a public blockchain as opposed to a private or consortium blockchain (on the distinction, see Mirchandani, 2018, pp. 1211–1213).

In a private or consortium blockchain, there is one or more private or hybrid organisation(s) responsible for overseeing the governance of the blockchain platform, determining, for instance, who will be the authorised nodes to enter information into the blockchain or to validate it. It may also be able to shield this information from the public eye. Examples involve, for instance, a financial institution that records

https://doi.org/10.1017/S1744552322000465 Published online by Cambridge University Press

information in a decentralised ledger, but allows only its authorised internal branches to access and modify information contained therein. In those cases, the challenges involving data protection are not novel. There is a clear controller responsible for potential data protection violations, with the actual power to limit different parties' ability to access and insert data in the blockchain.

For that reason, this paper will focus on examining the challenges of data protection in a *public* blockchain, where anybody with the technical ability and infrastructure can become a node, able to store a copy of the digital ledger and to validate it. In a public blockchain, there is no need for permission to operate in the blockchain platform. This is the case of most cryptocurrencies – including Bitcoin and Ethereum. The challenges of linkability and reversibility – discussed below – are relevant specifically in a public blockchain.

2.2 The vulnerabilities of data in blockchain platforms

Notwithstanding the widespread claims about the enhanced data privacy in blockchain platforms (Posadas Jr, 2018, p. 23) or the possibilities to enhance privacy protection through the use of these technologies (Wirth and Kolain, 2018), they in fact present an inherently paradoxical nature regarding data protection (De Filippi, 2016).

On the one hand, one primary purpose of a blockchain is the promotion of users' data sovereignty (Herian, 2020, p. 157), eliminating intermediaries to protect the data flowing in this platform from the surveillance of states and corporations. On the other hand, however, data stored in blockchain platforms may be subject to two main vulnerabilities: linkability and reversibility (European Union Blockchain Observatory Forum, 2018, p. 21).

The first challenge – linkability – refers to the possibility of unveiling the identity of the parties transacting in the blockchain platform through behavioural analytics. Most cryptocurrencies, to compensate for the lack of intermediation, disclose information about the transactions undertaken in non-permissioned blockchains (although not their specific content). In the case of Bitcoin, for instance, '[t]he public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone' (Nakamoto, 2008, p. 6). Similarly, smart contracts running on Ethereum are publicly visible (Etherscan, n.d.; Oliva *et al.*, 2020).

Based on the public information about transactions undertaken in the blockchain, several companies in the market offer data analytics services to identify who is behind a Bitcoin account – for instance – by linking an anonymised 'public key' in the ledger to a real entity or person (Elliptic, 2020). Public keys are the 'usernames' that users of blockchain platforms and applications utilise in their activities in the ledger and which are normally visible to all. They are composed of strings of letters and numbers that, in themselves, do not reveal the identity of the person/entity behind it. When combined with the private keys, they allow access and management of the data contained in the blockchain to be unlocked for its user.

Chainanalysis is one of the many blockchain analytics companies promising to promote cybersecurity by offering an '[i]nvestigation software that links real-world entities to cryptocurrency activity' (Chainanalysis, 2021). Through the combination of meta-data, which include 'on-chain and off-chain data such as location, KYC [know-your-customer] policies, counterparties, and news', it becomes possible, in many cases, to unveil the identity of the parties to a blockchain transaction, and especially for authorities with access to information provided by intermediaries (such as coin exchanges) that may be legally mandated to provide information about blockchain transactions (Snyder, 2021).

While the level of transparency in each blockchain application can be modulated, transparency is often deemed important for the meaningful co-ordination of the different parties in the blockchain, with the creation of a single shared source of truth.

While the further development of technical tools could allegedly have the potential to undermine these risks, creating computational methods to achieve consensus among the nodes without them being able to uncover the transactional data (see section 3), in its current state, it is unclear whether these methods can fully anonymise parties in the blockchain. Even if they could, however, it is questionable whether this would be desirable from a policy perspective.

https://doi.org/10.1017/S1744552322000465 Published online by Cambridge University Press

The second main challenge for privacy protection in the blockchain – reversibility – refers to the dangers of having the data stored in the blockchain, most often pseudonymised through encryption or hashing, reversed to its original version and thus becoming visible to third parties. Since the information registered in the blockchain in principle cannot be deleted, someone that becomes a node, for instance, could potentially have access to the underlying data in the distributed ledger, even though most likely in encrypted or hashed form. Reversing hashing or encryption, however, may not be an unachievable task for skilled hackers depending on the specifics of the technology used – rather than an impossibility, this is a matter of the level of sophistication required to perform this reversion (European Union Blockchain Observatory Forum, 2018, p. 22). This circumstance becomes clear when examining how data are stored in the blockchain.

There are three main ways to store data in a blockchain: in plain text, in encrypted form or in hashed form (European Parliament, 2019, p. 28). A blockchain platform will only store data in plain text if it is meant to give full access to its participants about the information contained therein – such as in a blockchain registering real estate ownership, expected to be available to the public. Otherwise, this solution is at odds with privacy and requires excessive storage space. For that reason, information is frequently either encrypted or hashed in the blockchain (Jimenez-Gomez, 2019, p. 335).

Encryption converts plain text into unreadable cyphertext, which can be reversed to its original form through a key. Blockchain mostly uses asymmetric encryption (involving a pair of public–private key cryptography). The public key is the equivalent of a pseudonymous 'username' (normally a long string of letters and numbers) that can be shared publicly without revealing someone's identity and to whom data can be sent and encrypted. The data, however, can be only decrypted to its original form through a private key, which works as a 'password' for its owner. The private key is what grants access to the data encrypted in the blockchain. Encryption is thus designed as a two-way reversible technique.

Hashing, instead, is a designed to be irreversible. It consists of the creation of a unique hash value – a string with a fixed number of letters and numbers – which is the representation of data of whatever length. Through a hashing algorithm, any amount of data can be converted into this unique hash digital signature. This mathematical conversion undertaken through an algorithm (hash function) is not reversible. For any similar input, a similar output (hash value) is generated. Even a minimal modification in the underlying data would result in a completely different hash value, clearly identifying whenever the data have been tampered with.

Despite the contributions to promote privacy, the security of encryption and, to a lesser extent, hashing techniques, is not clearly considered sufficient to ensure privacy. The EU Observatory Report specifically claims that encryption is not considered to promote anonymisation and claims that 'techniques used today may be cracked in the future' (European Union Blockchain Observatory Forum, 2018, p. 21). In relation to hashing, the situation is more nuanced, with the risks of reversibility being considered in relation to the specifics of the technology employed. If the dataset is relatively small, however, it may be possible to reverse it through a 'brute force attack' – requiring the use of additional techniques to ensure the security of the hashing (Ibanez *et al.*, 2018, pp. 8–9). With the advances of quantum computing, nevertheless, the potential to reverse hashing may be expanded even to large datasets.

In sum, currently data protection is needed in permissionless blockchains.

2.3 Challenges for implementing data protection in the blockchain

There is a growing literature about the challenges of implementing data protection rules in blockchain platforms and applications, under the GDPR and other data protection regulations.

Currently, the prevailing understanding is that the public keys and transactional data stored in the blockchain will often be considered personal data and, thus, subject to the GDPR (for an overview, see Finck, 2018a, pp. 91–99). In any case, this should be a case-by-case analysis – as in some situations non-personal data may be involved – for example, climatic information (European Union Blockchain Observatory Forum, 2018, p. 28). Under Article 4(1) GDPR, data are to be considered

https://doi.org/10.1017/S1744552322000465 Published online by Cambridge University Press

personal when they relate to 'an identified or identifiable natural person', through reference not only to its name, but also to identifiers such as location data, online identifiers or other factors that allow revealing the subject's identity. The prevailing understanding is that encrypted or hashed data in the blockchain constitute pseudonymised data – which may be reversed or linked with other metadata to reveal the parties' identity (European Union Blockchain Observatory Forum, 2018, pp. 29–31).

While the current state of affairs indicates the importance of implementing data protection in blockchain applications, the compatibility of the inherent architecture of blockchain technologies with data protection rules has been the subject of controversy in the recent past, not only in the context of the European GDPR, but also in the context of the California Consumer Protection Act (CCPA) (Alza, 2020), the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) (Walters, 2019) and beyond (INATBA Privacy Working Group, 2020). The most recently enacted regulations on this topic lack any specific rules regarding blockchain technologies. While the relevant statutes were meant to be technologically neutral, challenges remain unanswered, leading to the claim that '[b]lockchain technology is on a collision course with EU privacy law' (Meyer, 2018).

The implementation of the data protection rules to blockchain encounters two main obstacles. First, there is no clearly identifiable controller liable for privacy violations in permissionless blockchains (Schellekens, 2020).

Under Article 4(7) GDPR, the data controller is the natural or legal person who 'determines the purposes and means of the processing of personal data'. Controllers are expressly responsible towards the data subject for any potential data protection violations under Article 82 GDPR.

The determination of the controller can be challenging and must be performed case by case. It may sometimes be defined by law, while in other situations it will be determined according to the factual influence of the relevant entity in determining the purpose and influencing the means of processing (Finck, 2021, p. 334). Judicial authority and regulatory guidance, however, established a low threshold for someone to be considered the controller – with an influence in determining the purpose coupled with a minimal influence regarding the means of processing being considered sufficient for that purpose (Finck, 2021, pp. 333, 335). Given that data are nowadays processed by many actors, across 'data supply chains' (Voss, 2020), there may be many actors who could potentially be considered controllers.

In most cases, BigTech in the Internet will be considered controllers (De Filippi, 2016). Activities in the Web are typically organised through centralised platforms that will be considered the controllers, liable for potential data protection breaches in that platform and with the ability to access and control the data as may be necessary to comply with data protection rights. However, given the low threshold under the current law, there is a true pulverisation, in which even data subjects can sometimes be considered controllers (Finck, 2021, p. 338). In many situations, there may be more than one controller or 'joint controllership', creating a difficulty in determining who is liable and should be responsible for safeguarding data protection.

In a blockchain platform particularly, identifying the controller is challenging. One of the crucial features of blockchain technologies is their decentralised nature. The insertion of the data or any 'block' into the chain depends on the validation of the process by all or by a specified number of nodes in the network through a consensus protocol (Schellekens, 2020, pp. 216–217). This is particularly applicable to public blockchains. The information about the transactions – even though pseudonymised or encrypted – is often openly available for the public. There are challenges then to establish who the data controller will be.

The second main obstacle for the implementation of data protection in the blockchain is its allegedly 'immutable' character (Moerel, 2018, pp. 831–832). The GDPR contains different provisions that could be deemed incompatible with this immutability. On the one hand, the GDPR establishes principles of purpose minimisation (Art. 5(1)(b) GDPR), data minimisation (Art. 5(1)(c) GDPR) and storage limitation (Art. 5(1)(e) GDPR) of data (European Union Blockchain Observatory Forum, 2018, pp. 65ff.). Controllers and processors of data should maintain only the data that are crucial for the purposes of data processing and ought to minimise the data retained. Since the blockchain

https://doi.org/10.1017/S1744552322000465 Published online by Cambridge University Press

is designed to permanently store the information contained in the blocks – to guarantee trustworthiness – it would be difficult to comply with such principles.

On the other hand, the GDPR established that, under particular circumstances, data subjects have a right to rectify inaccurate data (Art. 16 GDPR) and a right to the erasure of data (or right to be forgotten, established in Art. 17 GDPR) (European Union Blockchain Observatory Forum, 2018, pp. 72ff.).

If there are no technical means to rectify and erase data from a blockchain, these might render data subjects' rights unenforceable, even if the violations are acknowledged. Both the ever-growing size of a blockchain and its distributed nature create an obstacle to limit the storage of users' data.

A blockchain, however, is not inherently immutable. In practice, a modification would be possible if a majority of nodes in the blockchain network (in a '51 per cent attack') agree on a particular modification of the previous blocks by creating an alternative chain (Werbach, 2018, pp. 46, 100ff.). The challenges to obtain such a majority, however, turn this into an unlikely occurrence. Nevertheless, that is possible and has already occurred in some cases (see section 4).

In addition to that, the geographical dispersion of blockchain users and miners brings additional challenges, since the international transfer of data is subject to different legal requirements, according to the applicable regulations. According to Statista, as of January 2022, the Bitcoin mining hash rate was divided among many countries (Statista, 2022). Ethereum also has a significant dispersion of its nodes around different countries (Ethernodes.org, 2022).

Since there is currently no global legal framework governing international transfers of data, what exists instead are different (geopolitical) models of data protection regulation. Both the GDPR and the California Consumer Privacy Act allow for the extra-territorial effect of their rules whenever data of their citizens are being processed (Voss, 2020, pp. 494, 498). In addition, China and Russia have 'data localisation' laws establishing that the data collected in their territory cannot but be stored by entities located in their territories, with some exceptions (Voss, 2020, p. 501). These different geopolitical models co-exist and sometimes require companies to fulfil different requirements at the same time.

The GDPR regulates international data transfers. Apart from the data flowing from the few countries with which the EU already has made 'adequacy' decisions or the US, where there is a 'Privacy Shield' in place which facilitates certifying that certain companies have an EU-adequate level of data protection, data transfer may be challenging. Under the GDPR, as interpreted by the relevant case-law, all entities with their 'main establishment' in the EU must comply with the GDPR, as well as those processing data of subjects located in the Union, even if the companies are located abroad (Voss, 2020, pp. 494–497). In the context of an economy organised in data supply chains, data may in practice flow through different jurisdictions – and specially in the case of blockchain applications, due to the geographical dispersion of nodes throughout the world. Each of these companies must then comply with the GDPR. The controller(s) is/are responsible for monitoring the different companies in the data supply chain, through contractual and governance instruments (see Art. 28, IV GDPR in conjunction with Art. 82 GDPR). All of that creates a very complex framework for monitoring data compliance only under the GDPR. When other laws potentially apply, this framework may become even more challenging.

In sum, the data protection literature has often considered the GDPR inadequate to regulate blockchains or sought to envision potential legal and technological adjustments to address the discussed challenges. The discussions often revolve around how to design GDPR-compliant blockchain applications.

3 Compliance technologies for privacy in the blockchain

This section surveys the main privacy-compliance technologies for blockchain technologies (Feng *et al.*, 2019; Satybaldy and Nowostawski, 2020; Wang *et al.*, 2020), identifying their limitations in implementing data protection, but also unveiling the crucial policy and legal decisions implicitly made when a particular technological design and form of implementation is adopted. These are

https://doi.org/10.1017/S1744552322000465 Published online by Cambridge University Press

often eclipsed by a techno-regulatory discourse about the potentialities of privacy-compliance technologies.

Overall, they have two main objectives: to ensure users' anonymity and to erase or make unavailable the data stored in the blockchain.

A first group of compliance technologies (Table 1) seeks to obfuscate the data in the blockchain, particularly users' public keys, with the objective of anonymising transactions – or rendering the identification of the parties involved difficult. Most blockchain platforms use asymmetric encryption to safeguard parties' identity. Through the use of blockchain analytics, however, this information can

Table 1. Privacy-compliance technologies promoting anonymity

Number	Technology	Description	Applications/benefits
1	Zero-knowledge proof	Allows the verification of a certain blockchain transaction by providing a binary true/false answer, without requiring access to the underlying information	Zcash; Zerocoin; ensuring anonymity and preserving confidentiality
2	Stealth address	Generation of a stealth address, to be used in a one-time transaction, with the hashing of one-time keys	Anonymity
3	Ring signature	Transactions are hidden through other transactions; one transaction is associated with a private key that is in turn connected to several public keys, creating obstacles to identify which of them initiated the transaction	Cryptonote; Monero; Anonymity
4	Homomorphic encryption	Allows different operations on encrypted data without the need to decrypt them in the process. An external or third party could be given the task of processing the sensitive data contained in the blockchain without having to decrypt it to achieve that objective	Confidentiality
5	Secure multiparty computation	Parties jointly agree to a multiparty computation function that operates without the need to disclose the inputs of any of the individuals	Simulation experiments with currency transfers and common smart contracts
6	Trusted execution environment	A secure, trusted, isolated area of software with enhanced confidentiality and integrity	Data security and integrity; Intel SGX
7	Commitment schemes	Mechanism through which a party maintains a piece of data secret, but commits to it by disclosing a hash of it	Anonymity; Ring CT; Monero
8	Adding 'noise' to the data ('mixing' services)	A number of transactions are grouped together, in a way that makes it difficult to identify the sender and recipient of each transaction	Bitcoin and Ethereum; recognised by Working Party Article 29 as a potential anonymisation technique

Sources: Feng *et al.*, 2019; Satybaldy and Nowostawski, 2020; European Union Blockchain Observatory Forum, 2018; Wang *et al.*, 2020.

https://doi.org/10.1017/S1744552322000465 Published online by Cambridge University Press

be combined with meta-data to arrive at the real identity of the parties (Feng *et al.*, 2019, pp. 48–49). This group of compliance technologies seeks ways to render the deployment of such analytics techniques difficult.

Perhaps the most disseminated technology applied for that purpose is the so-called zero-knowledge proof (Morais *et al.*, 2019), employed by cryptocurrency Zcash (Harikrishnan and Lakshmy, 2019). It allows for the system verification of the validity of a certain transaction, without revealing the underlying information, thus concealing the addresses of the individuals transacting. Through a sophisticated technological operation, the system evaluates a series of unlinkable pieces of information that are used to indicate a high probability that certain information is true – such as the identities of the parties and the features of a transaction – without the need to reveal them in the blockchain. Despite the benefits of this technology, there are still technical discussions regarding whether it can effectively anonymise transactions in the blockchain or whether it simply renders them more difficult to uncover. In addition, it presents other limitations, such as requiring more computing power, which results in more costs and infrastructure needed to apply this technique (Peng *et al.*, 2021, p. 304). It has also been questioned whether, with the advancements of quantum computing, zero-knowledge proof will become obsolete or easy to circumvent. Others have claimed that it is only a matter of time before these technologies become sophisticated enough to effectively anonymise the data. Table 1 presents techniques with the potential to anonymise parties and transactions in the blockchain.

A second group of compliance technologies (see Table 2) aims at limiting access and/or erasing the data contained in the blockchain, with the purpose of complying with the principles of the purposive use of data and data minimisation and with data subjects' rights to erase or rectify data. Perhaps the most-discussed technology in that category is that of storing data off-chain and simply leaving on-chain a hash link through which the information contained offline can be accessed (Finck, 2018a, pp. 94ff.). Certain security protocols are established to ensure that this off-chain database cannot be tampered with, which include the possibility of reintroducing an intermediary party to verify the data stored off-chain (Pinto, 2019). In this way, by storing information off-chain, the data are not contained in the blockchain nor replicated throughout the nodes, ensuring the purposive use of data, its minimisation and also the possibility of making it unavailable (some would consider that equivalent to erasing data). At the same time, however, by storing information off-chain, one of the main benefits of the blockchain platform is lost: a shared trust source. The blockchain enhances confidence through the fact that each of the nodes contains the entire blockchain database. If one node is compromised, all other nodes still contain the entire database, which can be verified. However, if the replicated information across the different nodes is simply a hash link to a different non-distributed database, the level of confidence in this information is undermined.

Based on a combination of privacy-enhancing technologies, a number of privacy coins have been deployed in the cryptocurrency market (*The Legal Examiner, 2021*). Privacy coins are cryptocurrencies that are claimed to ensure anonymity or at least be more protective of the identity of the parties in the blockchain and to obfuscate information about the transactions undertaken through it. Table 3 presents the main privacy coins in the cryptocurrency market and the main technologies used.

The description of compliance technologies reveals how privacy-by-design can contribute to establish blockchain applications where data protection principles can be upheld. At the same time, these technologies present limitations and embed different legal and policy choices, sometimes neglected in the academic debate.

At the outset, current state-of-the-art compliance technologies are not widely considered effective to promote data protection principles – even though they are seen as promising in the mid-term (European Union Blockchain Observatory Forum, 2018, p. 23). For each of the different privacy-compliance technologies, there are related disadvantages (see Table 2 in Feng *et al.*, 2019, p. 56). For instance, there are ongoing concerns whether the different anonymisation techniques can reliably protect the identity of users when data analytics techniques are used (De Filippi, 2016, p. 15). Similarly, a potential node who has access to the whole database could seek to reverse the encryption or hashing of the underlying information. It has been demonstrated that both encryption and hashing

https://doi.org/10.1017/S1744552322000465 Published online by Cambridge University Press

Table 2. Privacy-compliance technologies: focus on erasure and data minimisation

Number	Technology	Description	Benefits and applications
1	Storing data off-chain	Personal data are not stored in a blockchain, but off-chain and available through a hash link in the blockchain	Data minimisation; erasure of data; however, limits the benefit of using blockchain as single shared source of truth
2	Editable blockchain	Information underlying a block can be edited using a 'chameleon hash', where the change in the information does not alter the resulting hash, maintaining the coherence of the blockchain. The responsibility for the changes/ corrections would have to be in the hands of a single entity or to be decided through a strict management procedure as a way to maintain trust in the process	Accenture (patent); implementation of right to be forgotten, right to rectification/deletion in the blockchain
3	Limited ledger storage	After verification, the entire ledger is stored only in one or a few nodes, with the remaining nodes being required to delete the information contained in the ledger	Limit storage data; confidentiality; economic advantages (saving storage capacity and energy consumption)
4	Pruning	When verifying new blocks, nodes do not download the entire historical transactions; instead, they download only the blockchain headers and check up to the last 100 blocks. Ancient, unused blocks are not checked, but remain stored in a few 'archive' nodes	Data minimisation and less required storage capacity
5	Blockchain identity management	No personal data are stored at all in the blockchain, which is used only for self-sovereign identity management. Personal data of individuals are stored off-chain and made available, for a limited scope and time, upon authorisation of individuals when needed to prove their identity	Anonymity; confidentiality; data minimisation

Sources: Feng *et al.*, 2019; Satybaldy and Nowostawski, 2020; European Union Blockchain Observatory Forum, 2018; Wang *et al.*, 2020.

have certain vulnerabilities that could allow the reversibility of the hashed or encrypted data, thus uncovering them.

A first crucial issue, therefore, is whether privacy coins and the different anonymisation tools mentioned in this section can be considered as rendering anonymous the data contained in the blockchain for the purposes of the GDPR. If they were to achieve this objective, the GDPR would not be applicable to the concerned blockchain applications, since no personal data would be involved whatsoever. At the current stage, it is unclear whether privacy coins and anonymisation tools will be considered sufficient to render data anonymous under the GDPR (Finck, 2018b, pp. 28–29). Even European data protection authorities have already publicly acknowledged the uncertainty about how anonymity ought to be evaluated (Burt *et al.*, 2021). However, some positive indication was given by the Article 29 Working Party concerning the potential of techniques 'adding noise to the data' to effectively anonymise data, if used in conjunction with other technical means (Finck, 2018b, pp. 28–29). In any case, this is not a decision that should be made by developers in isolation nor by groups of experts insulated from the public debate. Given the continuous risks involved, these discussions must consider

https://doi.org/10.1017/S1744552322000465 Published online by Cambridge University Press

Table 3. Privacy coins

Name	Description	Technology used
Zcash	Seeks to hide both personal and transactional information, such as cryptocurrency addresses and the number of transactions undertaken. Allows the option to make some transactions fully public or to turn some aspects of the transaction private and others public	zk-SNARKs (zero-knowledge protocol)
Monero	Biggest market cap among privacy coins. Seeks to hide both addresses of senders and information about transactions	Stealth addresses and ring signature; RingCT
Verge	Encrypts personal addresses through I2P and then sends them through TOR to a distributed network, hiding IP addresses	I2P and TOR
Dash	Users are given the option to make their transactions public or private. Different transactions are combined into a single transaction, and then a particular amount is sent to each recipient	CoinJoin Method (makes identification more cumbersome but not considered a fully anonymising method)
Beam	Eliminates the need for any addresses, turning all transactions fully private	Mimblewimble (MW) Protocol

Sources: Investopedia, 2021; *The Legal Examiner*, 2021.
TOR, the onion routing; IP, internet protocol address.

the level of privacy risks that are to be accepted in different situations. Still, even if they are not considered to render the data anonymous, still these technologies can contribute to compliance with data protection principles – as in the case of tools allowing deletion of information accessed through the blockchain, which help to comply, for instance, with the right to be forgotten.

Second, in the deployment of these different technologies, there is an inevitable trade-off between values, principles or even technical capabilities. This technical trade-off is visible in the case of the Zcash coin, a cryptocurrency aimed to be privacy-enhancing, which cannot, however, support smart contracts, as it lacks technical capabilities for that purpose. A trade-off concerning values is also visible when compliance technologies achieve such a high degree of anonymisation that they may incur risks that the technology may be used for illicit transactions (such as money laundering) and to evade any kind of regulation. There seems to be a prevailing understanding that a blockchain needs to be – at least to some extent – regulated to prevent money laundering and illegal transactions. To achieve that purpose, the anonymisation of the parties cannot be complete (Hacker *et al.*, 2019, pp. 31–32). There must be some point of access through which the identity of the parties can be ascertained – through a governance practice, through an intermediary such as a Bitcoin wallet or through the use of certain technology that can reveal someone's identity.

This debate is already taking place in relation to privacy coins, which are banned in countries such as Japan and South Korea as they are seen as instruments to circumvent governmental regulations (NewsBTC, 2021). In other countries, such as the US, it may be possible to adjust privacy coins to the prevailing KYC and anti-money laundering regulations – but there are discussions ongoing on the possibility of outlawing them in the near future (James, 2018). For that reason, some coin exchanges have already decided to ban privacy coins from their platforms (Nasdaq, 2021).

A similar trade-off occurs in relation to technologies aiming at the minimisation of data in the blockchain. The more inaccessible or minimised the data are in the blockchain, the lower the level of confidence that can exist in a shared source of truth, as previously mentioned. Technology can always evolve to minimise those risks as it becomes more sophisticated – but in the end, that will involve a choice as to what values or principles will be prioritised over others.

https://doi.org/10.1017/S1744552322000465 Published online by Cambridge University Press

Third, even if these technologies continue to evolve from their current state-of-the-art to become more sophisticated and reliable in promoting data protection, in a similar way, hacking techniques, meta-analytics techniques, etc., will continue to develop, continually raising the bar of what compliance technologies must achieve to ensure the protection of privacy. One significant example concerns the developments of quantum computing, which some fear may disrupt the potentialities of technologies such as hashing or zero-knowledge proof in anonymising parties and transactions. In other words, there will be a continuous tug of war between the capabilities of compliance techniques and competing techniques aiming to circumvent them. Even if all-protective technologies were to be developed, it is likely that the costs of the most efficient ones would be higher and only become available to a few select companies in the market.

As compliance technologies to ensure data protection in the blockchain reveal their limitations, it is questionable how a more social, trust-based or human-centred perspective of blockchain technologies could contribute to address the existing challenges.

4 A social, trust-based or human-centred perspective to the blockchain and its implications concerning privacy

The concept of trust has been largely studied across law and the computer and social sciences, with different meanings ascribed to it even within a same discipline. In this paper, we distinguish between two concepts: trust in the technical system, which is deterministic and independent from human action; and trust as reliance on human individuals, regardless of technological elements (Becker and Bodó, 2021). This correlates with two notions of blockchain: one in which it constitutes an order that is (at least relatively) self-sufficient and the other in which it is more deeply embedded in the political and legal realm (Hacker *et al.*, 2019, p. 13).

A first trend of studies on blockchain technologies highlighted how they can substitute the need for trust in the human and social element – thus creating a form of trustless trust (Harz and Boman, 2019), emphasising how (crypto)economic and behavioural incentives propel most of the actors in the platform to reliably behave according to the blockchain rules. In this context, trust subsists only as reliance in the technical reliability of the blockchain technology – that is, 'the security of computer systems, them being free of errors, and bugs, working as intended and advertised' (Becker and Bodó, 2021, p. 3). The blockchain is therefore envisioned as an order (almost) apart from the conventional legal system.

A second trend of studies has sought to unveil how trust (or confidence) remains an important element for the proper functioning of the blockchain. In that sense, De Filippi *et al.* have emphasised how some form of 'distributed trust' in the behaviour of the different actors in the blockchain remains crucial to ensure the proper functioning of its applications (De Filippi *et al.*, 2020, p. 63).

In that sense, different studies highlighted the importance of trusting in the conduct of different actors in the blockchain platform, such as miners, software developers or cryptocurrency exchanges (Walch, 2019). In a similar direction, different authors claimed that reliance on human-interpreted institutions of law will continue to have a relevant role in a significant number of blockchain applications (Werbach, 2018; Yeung, 2019).

Despite the different views on this social perspective of the blockchain, they converge to the idea that there is need for reliance on human-mediated legal institutions to govern the blockchain protocol. How the legal or governance framework should be established, however, remains an open question (De Filippi *et al.*, 2020, p. 11). The following subsections examine how such a human-centred perspective could be envisioned to enhance data protection in the blockchain.

4.1 Designing compliance technologies for a blockchain with humans in the loop

The use of code-driven technologies is promoted based on the premise that they will be more efficient than human beings in solving different types of problems. This techno-regulatory perspective often leads to designing machines with the purpose of eliminating or minimising the human role. It

https://doi.org/10.1017/S1744552322000465 Published online by Cambridge University Press

seeks to create a 'legal by design' technological architecture supposedly inherently compliant with laws (Lippe *et al.*, 2015).

This perspective has been criticised for disregarding the importance of maintaining human agency in decision-making to uphold the rule of law (Hildebrandt, 2020b, pp. 79ff.). In relation to blockchain technologies or other code-driven technologies, this challenge can be even more prominent, since there is a conflation of rule, enforcement and adjudication (Hildebrandt, 2020a, p. [14]). In other words, once a certain blockchain/smart contract operating on a blockchain platform is coded to operate in a certain way, it will automatically perform these tasks without the need or sometimes even the opportunity for human supervision. In itself, the notion that a contract or regulation could have a single, unchallengeable meaning that could be enforced automatically represents a regression to a purely formalistic perspective of the law (Verstraete, 2019).

The discussions about the use of blockchain technologies often employ premises based on this techno-regulatory perspective (Herian, 2019, p. 12). This is often observable in the discussions about privacy in the blockchain, which often impliedly follow the notion that technologies will eventually become sophisticated enough to ensure full anonymisation or to allow a secure storage off-chain of data in the blockchain, ignoring important policy decisions behind the technology architecture that will significantly affect the different actors in the blockchain and beyond. As mentioned, a complete or high degree of anonymisation – if possible at all – could lead to the impossibility of regulatory oversight on the blockchain. Similarly, the possibility of storing data off-chain – instead of in the blockchain – may undermine the trustworthiness of the shared ledger. If the off-chain storage of data proves to be completely safe, it may be questionable whether there is a need for a decentralised blockchain platform at all. The decisions on how to frame these technologies have significant effects that sometimes seem to be entirely ignored in the search for a perfectly efficient technology.

Evoking Hildebrandt, the notion of 'legal design' should give way to the notion of 'legal protection by design' (Hildebrandt, 2020b, pp. 79ff.). The latter, instead of seeking to substitute or eliminate the need for the human in these technologies, seeks to frame their participation to make these technologies accountable. In the context of code-driven platforms, such as the blockchain, this could mean both the participation of the relevant stakeholders in the design of the blockchain and also designing a technology that includes the 'human in the loop'.

The regulation of blockchain platforms and the applications operating on top of them should somehow involve the participation of the affected participants and stakeholders particularly when it affects a significant number of actors, who sometimes may not even be aware of these potential effects (Herian, 2019, p. 2), such as cryptocurrencies largely used by a significant number of investors and consumers, and open to the general public to acquire. In such a case, privacy decisions have wider effects on investors, consumers and citizens in general, irrespective of whether they are public or private, and there should be forms to include the participation of these actors or their representatives in the privacy design choices in the blockchain. Insufficient data protection is only one of the harms to which the public may be exposed, among others such as digital identity theft or fraudulent investment – around 78 per cent of Initial Coin Offerings (ICOs) offered in 2017 were actually scams (Benedetto Neitz, 2020, p. 189).

If the blockchain platform involves one group of companies and has only repercussions within that group, it may be acceptable to restrict such participation to the participants of the group or to a chosen controller, as in blockchain applications used to monitor companies' supply chains (Gaur and Gaiha, 2020).

The certification of blockchain platforms could play a significant role in their regulation. Certification could include the requirement to involve discussions with non-governmental bodies or entities representing consumers or different categories of citizens in the design of the technological architecture of the platform, including the crucial decisions on privacy in a particular environment. Core developers should not determine in isolation what is privacy.

In contexts in which it is more evident how compliance technologies should be structured, such matters could be governed by regulation. For instance, it seems widely accepted that privacy could be disregarded in land registries stored in a blockchain. In this case, it is important to maintain the full transparency of the identity and the assets registered for the wider public.

https://doi.org/10.1017/S1744552322000465 Published online by Cambridge University Press

Besides participation in the design, another important issue is how to design blockchain applications involving human participation, balancing concerns involving privacy and accountability of potential illegal activity. We discuss this issue in the context of a technical project for an improved form of the privacy coin Monero.

4.1.1 The case of 'traceable Monero': balancing anonymity and accountability

Monero is a cryptocurrency implementing privacy-enhancing techniques, with the purpose of anonymising users and their respective transactions (specifically RingCT, Ring signatures, one-time stealth addresses and Kovri; see SerHack and the Monero Community, 2018, p. 60). The challenge of Monero – similarly to other privacy coins – is that enhancing anonymity may pave the way for illegal activities (such as money laundering) to be performed with this token. Since the parties' identity and their transactions become shielded by the privacy-enhancing techniques employed, regulators and enforcement bodies might become unable to make accountable users using cryptocurrency for illegal purposes.

Monero has in fact been used on different occasions to perform illegal activities (Hannah Murphy, 2021). This challenge has led the technical community to discuss how to balance privacy-enhancing techniques with the ability to make accountable users employing cryptocurrency for illegal purposes. Instead of idealising the potentialities of anonymisation techniques, the technical discussions have sought ways to balance anonymity with the need to ensure accountability in the blockchain.

How Monero enhances privacy. As with Bitcoin, each user in Monero has a public key (koe *et al.*, 2020, p. 44). Whenever coins are transferred to a public address, however, the transactions are not recorded as sent to a particular public key. Instead, a one-time stealth address is generated and the public record indicates that a transaction was made to this address. Therefore, in principle, it is not possible through data analytics to identify the party behind an account or related patterns of an account, as the addresses used for receiving funds are unique and not used twice.

To verify whether funds have been received in the Monero blockchain, each user has to scan the public record with a 'secret view key', which can be used to reveal whether particular funds sent to a stealth address were addressed to a particular recipient (Monero.how, n.d.). However, no mention of the public keys is available in the public record. This feature creates the unlinkability of transactions to the user's particular public key.

In addition, Monero also uses a ring signature to prevent the sender from verifying whether the funds sent to a particular (one-time) address have been further spent/transferred (SerHack and the Monero Community, 2018, p. 67). Whenever funds are transferred, they are associated with a ring of other funds. Thus, it is not possible to identify from which sender they originated. Monero further employs an extension of the ring signature technique (called RingCT), which also hides the amount of funds transferred. This is undertaken 'by applying a mathematical function to all funds such that public observers can see that the transactions are legitmate [sic], but only the sender and receiver can know the actual amounts (Monero.how, n.d.).'

Currently, Monero is also developing Project Kovri – to hide users' Internet traffic when using Monero so that for passive network monitors it becomes unfeasible to detect that a user is in the platform (SerHack and the Monero Community, 2018, p. 71). This is achieved by encrypting Monero traffic and routing it through the Invisible Internet Project.

Even with the application of these privacy-enhancing technologies, empirical studies have already demonstrated that some technical vulnerabilities still persist and may allow, depending on their sophistication, the identification of the parties and their transactions – with continuing discussions on how to improve those aspects (Möser *et al.*, 2018).

The abuses involving Monero. The privacy-enhancing features of Monero have led it to be coined as 'the crypto of choice for cybercriminals' (Hannah Murphy, 2021).

https://doi.org/10.1017/S1744552322000465 Published online by Cambridge University Press

Several incidents surrounding Monero support this claim (Möser *et al.*, 2018, pp. 15–16). For instance, AlphaBay, considered the most prominent DarkNet after SilkRoad was shut down in 2013, used to accept Monero for its transactions (AlphaBay was shut down in 2017 after investigations and was relaunched in 2021). In the same vein, a group of hackers called 'The Shadow Brokers' offered hacking tools and services in exchange for payments in Monero.

These different incidents have led several trade platforms for blockchains to abolish the use of privacy coins such as Monero.

Potential technical solutions. Discussions are currently underway in the technical community as to how to combine enhanced anonymity with the need to revoke it to investigate potential fraud. There are three main ways to fulfil this objective.

First is through the analysis of the transactions in the blockchain, previously explored. This task, however, is much more challenging regarding Monero (and other privacy coins) due to privacy-enhancing techniques and the need for a significant amount of external information that would be required to discover someone's identity. An empirical study has estimated that around 62 per cent of transaction inputs in Monero are still subject to chain analysis, with the potential for uncovering identities and related transactions with this token (Möser *et al.*, 2018, p. 1). In some of the incidents previously mentioned, in fact, the parties behind Monero have been identified. If used by more sophisticated parties strategically adopting privacy-enhancing technologies, however, traceability might be significantly more difficult and costly.

Second, anonymity could be revoked if there is an intermediary party – as in a private or consortium blockchain – which oversees transactions and is able to check the information about the parties. Private or consortium blockchains, however, are not the focus of this paper, which instead is centred on examining permissionless blockchains.

Third, there are cryptographic tools that could potentially allow for selectively uncovering someone's identity or transactions in the blockchain. An example of such a system is 'Traceable Monero', which has been developed by a group of engineers (Li *et al.*, 2021). It proposes to adapt the Monero system so that, while it remains anonymous, a tracing authority is created, which is able to revoke the anonymity of the parties under certain circumstances. This tracing authority, however, is notably passive and optimistic, meaning that it only intervenes to revoke it when a formal investigation is required (Li *et al.*, 2021, p. 680).

This proposed improved form of Monero creates a mechanism through which a digital 'tag' is stamped to the one-time stealth address generated for a particular transaction concluded by a party (the tags will be different for each of the parties, even in the same transaction) (Li *et al.*, 2021, p. 684). The tag, which is encrypted, can be decrypted by an authority who possesses a private key with that capability. Once decrypted, the tag reveals the long-time public keys of the concerned party (Li *et al.*, 2021, p. 685).

Traceable Monero presents an effective possibility, through technical means, to balance anonymity and traceability, putting humans in the loop.

4.2 Contestability regarding privacy compliance in the blockchain

Legal regimes ensuring that blockchain platforms and applications are privacy-compliant must facilitate the enforcement of the rights of the aggrieved parties. The enforcement challenges regarding blockchain applications, however, may be significant.

Even though there is no specific precedent regarding privacy violations in blockchain platforms, under Article 82 GDPR, parties aggrieved by privacy violations under the regulation can obtain compensation for their material or non-material loss (e.g. the emotional distress caused by the leak of the data) (see e.g. *Google Inc. v. Vidal-Hall* [2015] EWCA Civ 311). Whenever companies do not voluntarily agree to the compensation, the claim may have to be brought to court. Typically, the monetary amount of the damage involved in many cases involving privacy in the blockchain may be too low to

https://doi.org/10.1017/S1744552322000465 Published online by Cambridge University Press

be taken by high-profile law firms and may be too cumbersome or costly to be proven by a single affected investor or consumer – especially those involving non-material loss.

Clearly, there is some degree of expertise required from the legal counsel initiating these claims that involve complex legal and technological issues. The costs to obtain such counsel, nevertheless, may be too high. A US firm with expertise in cryptocurrency litigation clarifies on its website that 'we generally limit the cases we take to those in which more than $200,000 is at issue' (Patterson Law Firm, n.d.) – pointing out that pro-bono or other alternatives should be sought for cases not falling above that threshold.

The rising number of class actions brought against cryptocurrency exchanges and issuers of tokens in the past few years – especially in the US – indicates the challenges to undertaking single suit litigation in this type of dispute (Zaslowsky, 2021; Reuters, 2020; Cointelegraph, 2021). Most of these class actions brought involved the claim that the cryptocurrency exchanges or issuers of tokens in ICOs failed to meet disclosure requirements under securities law, alleging that cryptocurrencies should be legally classified as security.

Consumers' ability to access justice, however, may be at risk. A recent empirical study involving the Terms and Conditions of 300 of the major cryptocurrencies and exchanges (Meshel and Yahya, 2021, pp. 212–213) indicated that, in disputes involving cryptocurrencies, there has been a slight (and statistically non-significant) preference for litigation over arbitration. For cryptocurrencies and exchanges opting for arbitral proceedings, in 53 per cent of the cases, there were clauses expressly prohibiting class proceedings, having been indicated as the crucial determinant for parties to choose arbitration over litigation (Meshel and Yahya, 2021, pp. 221, 231). In litigation, clauses prohibiting class litigation were less frequent (16.75 per cent) and were positively correlated with situations in which there was a choice of the venue of the litigation (Meshel and Yahya, 2021, pp. 243, 227).

In this context, it is important to ensure that the underlying legal framework facilitates class actions brought by a plurality of aggrieved parties in the blockchain, making it possible for individual stakeholders affected to join forces to make accountable the actor(s) potentially responsible for the privacy violations. It would be further important to ensure compliance that public entities or non-governmental organisations representing the interests of certain protected actors – such as consumers – may have the standing to propose class actions whenever they affect a significant number of actors. While this may not generally be an issue whenever the interests of business corporations are affected, they may be significant when other minor investors/consumers transacting in the blockchain are involved.

4.3 Finding out who is responsible or distributing liability in the blockchain platform

The establishment of a contestable, privacy-compliant framework also involves determining who will be responsible for potential privacy violations in the blockchain. Nevertheless, in the context of a narrative about a 'distributed', 'decentralised' blockchain platform, it has become difficult to identify who can be indicated as the controller responsible for potential privacy violations (Jimenez-Gomez, 2019, p. 311). This is perhaps one of the most-discussed aspects concerning privacy in the blockchain. The debate about what roles different actors retain in the blockchain involves a social perspective of the blockchain, where the human role has relevance.

It is often indicated that no single actor has the power to manipulate the blockchain – pointing out this as one of the major benefits of these platforms. This narrative has been questioned by studies emphasising that the decentralised nature of blockchain technologies has to be relativised (see Walch, 2019). In fact, there are several 'pockets of power' in different blockchain platforms in which a few select actors make decisions that have an influence throughout the network. Different cases involving the Bitcoin and Ethereum systems (potentially extendable to other platforms as well) demonstrate that particularly core developers and significant miners have such power (Walch, 2019, p. 52).

Core developers are a select group that have the 'commit keys' through which they can change the code repository of the blockchain platform. They can write code that will determine crucial policy

https://doi.org/10.1017/S1744552322000465 Published online by Cambridge University Press

choices in the blockchain – such as how expensive it is to participate in the system (Walch, 2019, p. 52). In different situations, core developers' decisions have been crucial in structuring or altering the structure of platforms. For example, in 2013, when an unexpected fork of the Bitcoin system occurred, with two different versions of the software, it was a select number of developers who decided which version of the software was legitimate and contacted the major miners in the system to persuade them to adopt such a version.

Miners with a relevant proportion of the mining power may also have a significant influence in the platform. It has been indicated that very few 'mining pools' in the Ethereum and Bitcoin platform held over 50 per cent of the mining power in these platforms. That would enable those mining pools, if they decided to act together, to perform a 51 per cent attack in a platform, rewriting the blockchain to obtain advantages, as was the case in relation to the platform Ethereum Classic, where a 51 per cent attack enabled an attacker to steal 1 million dollars.

Besides core developers and miners, other sites of power concentration may exist in the blockchain. For instance, it has been claimed that wallet exchanges – which may have the power to determine whether tokens should or not be listed for trading or holders of a significant number of tokens in platforms ('whales') – may have a disproportionate influence in the platform.

Most of these discussions, however, have not been neglected in the debate about liability for potential privacy violations in the blockchain.

Several suggestions have been proposed to determine who is the controller – liable for potential privacy violations in the blockchain. The French Commission Nationale Informatique & Libertés (CNIL) issued a report on the relationship between the GDPR and blockchain platforms (CNIL, 2018). The report suggested that participants of the blockchain platform entering data in the platform will be considered as controllers – whenever they are legal entities or are processing the data for professional purposes (thus excluding participants who process data for personal purposes). The example provided in the report of a participant that would be deemed a controller, liable for privacy violations, is that of a public notary who would insert the information in the blockchain platform (CNIL, 2018, p. 2). Notably, miners would not be considered responsible for violations, as they are not responsible for establishing the purposes and objectives of the data processing. The report also points out the possibility of the parties in the blockchain platform establishing who will be liable for potential violations.

The discussion about liability should be deepened to determine, under different circumstances, which parties are responsible for privacy violations in different scenarios. Regulation should establish as a requirement for the functioning of these platforms that an entity or party should be indicated as responsible for these potential data protection violations – which could be then reversed in each case considering the circumstances of the case.

5 Conclusion

This paper has critically examined the techno-regulatory narrative about the potentialities of privacy-compliance technologies in blockchains. Currently, the proposals to promote data protection in blockchains often revolve around how to establish an inherently GDPR-compliant design, implying that, upon further development, compliance technologies may be able to fully automate compliance without the need for human participation.

The paper counters this narrative with a social perspective of the blockchain and develops different proposals on how to ensure human participation and contestability regarding the privacy-compliance framework in the blockchain.

First of all, the paper refutes the prevailing dichotomic narrative between those who defend improving privacy-compliance technologies, for instance, to enhance anonymity, and those claiming that these types of technology should be banned by their potential to evade regulators and law enforcement. Instead, the paper argues that privacy should be envisioned in terms of levels of intensity or layers that may be more or less intense in different cases or circumstances. The Traceable Monero project was used as an example to demonstrate that there are ways to combine anonymity with regulatory

https://doi.org/10.1017/S1744552322000465 Published online by Cambridge University Press

monitoring, such as by creating an entity able to revoke the anonymity of parties and transactions in exceptional cases, when relevant investigations are ongoing.

Second, the paper defends the proposition that, whatever the layer of privacy adopted by a particular blockchain application, it should not – and cannot – escape incorporating human involvement. Such participation may be established at the design level – in the example of Traceable Monero, by creating an entity that can revoke anonymity to pursue potential fraudulent activities when investigations are ongoing. This form of participation can further happen *ex post*, by guaranteeing a legal framework that effectively allows for contestability of decisions related to privacy. From that aspect, it particularly defended the importance of guaranteeing the possibility for consumers to initiate class action claims related to privacy violations – a possibility demonstrated to be under attack in at least some jurisdictions. Effective contestability will also further require exploring the determination of the liable controller in the blockchain – a definition that in most cases still remains unclear.

Acknowledgements. None

Conflicts of Interest. None

References

Alza G Jr (2020) Blockchain & CCPA. *Santa Clara High Technology Law Journal* **37**, 231–255.

Becker M and Bodó B (2021) Trust in blockchain-based systems. *Internet Policy Review* **10**, 1–10.

Benedetto Neitz M (2020) How to regulate blockchain's real-life applications: lessons from the California Blockchain Working Group. *Jurimetrics* **61**, 185–218.

Burt A, Rossi A and Bourdillon S (2021) *A Guide to the EU's Unclear Anonymization Standards*. Available at: https://iapp.org/news/a/a-guide-to-the-eus-unclear-anonymization-standards/ (accessed 28 June 2022).

Casino F, Dasaklis TK and Patsakis C (2019) A systematic literature review of blockchain-based applications: current status, classification and open issues. *Telematics and Informatics* **36**, 55–81.

Chainanalysis (2021). *The Blockchain Data Platform*. Available at https://www.chainalysis.com/ (last accessed 15 September 2021).

CNIL (Commission Nationale Informatique & Libertés) (2018) *Premiers éléments d'analyse de la CNIL – Blockchain*. Available at: https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf (accessed 30 August 2022).

Cointelegraph (2021) *Five Proposed Crypto Class Actions over Unregistered Securities Dismissed in NY*. Available at: https://cointelegraph.com/news/five-proposed-crypto-class-actions-in-ny-over-unregistered-securities-dismissed (accessed 4 October 2021).

Daoui S, Fleinert-Jensen T and Lempérière M (2019) GDPR, blockchain and the French Data Protection Authority: many answers but some remaining questions. *Stanford Journal of Blockchain Law & Policy* **2**, 240–251.

De Filippi P (2016) The interplay between decentralization and privacy: the case of blockchain technologies. *Journal of Peer Production* **7**, 0–18.

De Filippi P, Mannan M and Reijers W (2020) Blockchain as a confidence machine: the problem of trust & challenges of governance. *Technology in Society* **62**, 1–14.

Elliptic (2020) *A Brief Guide to Analytics on Blockchain*. Available at: https://www.elliptic.co/blog/a-brief-guide-to-analytics-on-blockchain (accessed 4 November 2021).

Ethernodes.org (2022) *The Ethereum Network & Node Explorer*. Available at: https://ethernodes.org/countries (accessed 28 June 2022).

Etherscan (n.d.) *The Ethereum Blockchain Explorer*. Available at: http://etherscan.io/ (accessed 15 July 2021).

European Parliament (2019) *Blockchain and the General Data Protection Regulation: Can Distributed Ledgers Be Squared with European Data Protection Law?* Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf (accessed 13 August 2022).

European Union Blockchain Observatory Forum (2018) *Blockchain and the GDPR*. Brussels: EU. Available at: https://www.eublockchainforum.eu/sites/default/files/reports/20181016_report_gdpr.pdf (accessed 30 August 2022).

Fairfield JAT (2019) The human element: the under-theorized and underutilized component vital to foster blockchain development. *Cleveland State Law Review* **67**, 33–40.

Feng Q *et al.* (2019) A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications* **126**, 45–58.

Finck M (2018a) *Blockchain Regulation and Governance in Europe*. Cambridge: Cambridge University Press.

Finck M (2018b) Blockchains and data protection in the European Union. *European Data Protection Law Review* **4**, 17–35.

Finck M (2021) Cobwebs of control: the two imaginations of the data controller in EU law. *International Data Privacy Law* **11**, 333–347.

https://doi.org/10.1017/S1744552322000465 Published online by Cambridge University Press

Gaur V and Gaiha A (2020) Building a Transparent Supply Chain. *Harvard Business Review*, May–June.
Hacker P *et al.* (2019) Regulating blockchain: techno-social and legal challenges – an introduction. In Hacker P *et al.* (eds), *Regulating Blockchain: Techno-social and Legal Challenges*. Oxford: Oxford University Press, pp. 1–24.
Hannah Murphy (2021) Monero emerges as crypto of choice for cybercriminals. *Financial Times*, 22 June. Available at: https://www.ft.com/content/13fb66ed-b4e2-4f5f-926a-7d34dc40d8b6 (accessed 13 August 2022).
Harikrishnan M and Lakshmy KV (2019) *Secure Digital Service Payments Using Zero Knowledge Proof in Distributed Network*, 5th International Conference on Advanced Computing Communication Systems (ICACCS), Coimbatore, India, 15–16 March 2019, pp. 307–312. Available at: https://doi.org/10.1109/ICACCS.2019.8728462 (accessed 13 August 2022).
Harz D and Boman M (2019) The scalability of trustless trust. In Zohar A *et al.* (eds), *Financial Cryptography and Data Security, Lecture Notes in Computer Science*. Berlin and Heidelberg: Springer, pp. 279–293.
Herian R (2019) *Regulating Blockchain: Critical Perspectives in Law and Technology*. New York: Routledge.
Herian R (2020) Blockchain, GDPR, and fantasies of data sovereignty. *Law, Innovation and Technology* **12**, 156–174.
Hildebrandt M (2020a) A philosophy of technology for computational law. In Mangan D, Easton C and Sithig DM (eds), *The Philosophical Foundations of Information Technology Law*. published online 18 November 2020. Available at: https://osf.io/preprints/lawarxiv/7eykj/ (accessed 30 August 2022).
Hildebrandt M (2020b) Code driven law: scaling the past and freezing the future. In Deakin S and Markou C (eds), *Is Law Computable? Critical Perspectives on Law and Artificial Intelligence*. Oxford: Hart Publishing, pp. 67–83.
Ibanez LD, O'Hara K and Simperl E (2018) *On Blockchains and the General Data Protection Regulation*. Working Paper, EU Blockchain Forum and Observatory, 2018. Available at: https://eprints.soton.ac.uk/422879/1/BLockchains_GDPR_4.pdf (accessed 13 August 2022).
INATBA Privacy Working Group (2020) *Report on Data Protection Regulations Applicable to Blockchain Technology in Different Jurisdictions Worldwide*. International Association for Trusted Blockchain Applications. Available at: https://inatba.org/wp-content/uploads/2021/01/2020-12-Privacy-WG-Report-on-Data-Protection.pdf (accessed 13 August 2022).
Investopedia (2021) *6 Most Private Cryptocurrencies*. Available at: https://www.investopedia.com/tech/five-most-private-cryptocurrencies/ (accessed 18 November 2021).
James A (2018) Privacy coins are 'one of the greatest emerging threats to U.S. National Security,' states US congressman. *Bitcoinist*. Available at: https://bitcoinist.com/privacy-coins-greatest-emerging-threats-national-security/ (accessed 13 August 2022).
Jimenez-Gomez BS (2019) Risks of blockchain for data protection: a European approach. *Santa Clara High Technology Law Journal* **36**, 281–344.
koe, Alonso KM and Noether S (2020) *Zero to Monero: A Technical Guide to a Private Digital Currency for Beginners, Amateurs, and Experts*, 2nd edn. Available at: https://www.getmonero.org/library/Zero-to-Monero-2-0-0.pdf (accessed 13 August 2022).
Law Society of England and Wales (2020) *Blockchain: Legal and Regulatory Guidance*. London: The Law Society of England and Wales. Available at: https://www.lawsociety.org.uk/topics/research/blockchain-legal-and-regulatory-guidance-report (accessed 30 August 2022).
Leenes RE (2011) Framing techno-regulation: an exploration of state and non-state regulation by technology. *Legisprudence* **5**, 143–169.
Li Y *et al.* (2021) Traceable Monero: anonymous cryptocurrency with enhanced accountability. *IEEE Transactions on Dependable and Secure Computing* **18**, 679–691.
Lippe P, Katz DM and Jackson D (2015) Legal by design: a new paradigm for handling complexity in banking regulation and elsewhere in law. *Oregon Law Review* **93**, 833–852.
Meshel T and Yahya MA (2021) Crypto dispute resolution: an empirical study. *University of Illinois Journal of Law, Technology and Policy* **2021**, 187–256.
Meyer D (2018) *Blockchain Technology Is on a Collision Course with EU Privacy Law*. Available at: https://iapp.org/news/a/blockchain-technology-is-on-a-collision-course-with-eu-privacy-law/ (accessed 15 July 2021).
Mirchandani A (2018) The GDPR-blockchain paradox: exempting permissioned blockchains from the GDPR. *Fordham Intellectual Property Media & Entertainment Law Journal* **29**, 1201–1241.
Moerel L (2018) Blockchain & data protection – and why they are not a collision course. *European Review of Private Law* **26**, 825–851.
Monero.how (n.d.) *A Low-level Explanation of the Mechanics of Monero vs Bitcoin in Plain English*. Available at: https://www.monero.how/how-does-monero-work-details-in-plain-english (accessed 16 June 2022).
Morais E *et al.* (2019) A survey on zero knowledge range proofs and applications. *SN Applied Science* **1**, 946.
Möser M *et al.* (2018). An empirical analysis of traceability in the Monero blockchain. *Proceedings on Privacy Enhancing Technologies* 2018, 143–163.
Nakamoto S (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available at: https://bitcoin.org/bitcoin.pdf (accessed 30 August 2022).
Nasdaq (2021) *Bittrex to Delist 'Privacy Coins' Monero, Dash and Zcash*. Available at: https://www.nasdaq.com/articles/bittrex-to-delist-privacy-coins-monero-dash-and-zcash-2021-01-01 (accessed 4 November 2021).

NewsBTC (2021) An overview about privacy coins in 2021: what's ahead? Available at: https://www.newsbtc.com/sponsored/an-overview-about-privacy-coins-in-2021-whats-ahead/ (accessed 16 November 2021).

Oliva GA, Hassan A and Jiang ZM (2020) An exploratory study of smart contracts in the Ethereum blockchain platform. *Empirical Software Engineering* **25**, 1864–1904.

Patterson Law Firm (n.d.) *Cryptocurrency Litigation Lawyer & Litigation Law Firm – Chicago*. Available at: https://www.pattersonlawfirm.com/practice-areas/cryptocurrency-litigation/ (accessed 4 October 2021).

Peng L *et al.* (2021) Privacy preservation in permissionless blockchain: a survey. *Digital Communications and Networks* **7**, 295–307.

Pinto R (2019) Council post: on-chain versus off-chain: the perpetual blockchain governance debate. *Forbes*, 6 September. Available at: https://www.forbes.com/sites/forbestechcouncil/2019/09/06/on-chain-versus-off-chain-the-perpetual-blockchain-governance-debate/ (accessed 13 August 2022).

Posadas Jr DV (2018) The Internet of Things: the GDPR and the blockchain may be incompatible. *Journal of Internet Law* **21**, 1–29.

Reuters (2020) Cryptocurrency issuers, exchanges face U.S. class action lawsuits. Available at: https://www.reuters.com/article/us-cryptocurrency-usa-lawsuit-idUSKBN21O2I5 (accessed 13 August 2022).

Satybaldy A and Nowostawski M (2020) *Review of Techniques for Privacy-preserving Blockchain Systems*, Proceedings of the 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure, BSCI '20, Association for Computing Machinery, New York, NY, USA, 5–9 October 2020, pp. 1–9.

Schellekens M (2020) Conceptualizations of the controller in permissionless blockchains. *Journal of Intellectual Property, Information Technology and E-Commerce Law* **11**, 215–227.

SerHack and the Monero Community (2018) *Mastering Monero – the Future of Private Transactions*. LernoLibro. Available at: https://masteringmonero.com/book/Mastering%20Monero%20First%20Edition%20by%20SerHack%20and%20Monero%20Community.pdf (last accessed 13 August 2022).

Snyder S (2021) The privacy questions raised by blockchain. *Law360*, 14 January. Available at: https://www.law360.com/articles/1115579/the-privacy-questions-raised-by-blockchain (accessed 13 August 2022).

Statista (2022) *Bitcoin Mining by Country 2021*. Available at: https://www.statista.com/statistics/1200477/bitcoin-mining-by-country/ (accessed 28 June 2022).

Teperdjian R (2019) The puzzle of squaring blockchain with the General Data Protection Regulation. *Jurimetrics* **60**, 253–314.

The Legal Examiner (2021) Privacy coins 101. 23 September. Available at: https://www.legalexaminer.com/technology/crypto/privacy-coins-101/ (accessed 13 August 2022).

Verstraete M (2019) The stakes of smart contracts. *Loyola University Chicago Law Journal* **50**, 743–795.

Voss WG (2020) Cross-border data flows, the GDPR, and data governance. *Washington International Law Journal* **29**, 485–532.

Walch A (2019) Deconstructing 'decentralization': exploring the core claim of crypto systems. In Brummer C (ed.), *Cryptoassets: Legal, Regulatory, and Monetary Perspectives*. Oxford: Oxford University Press, pp. 39–68.

Walters N (2019) Privacy law issues in public blockchains: an analysis of blockchain, PIPEDA, the GDPR, and proposals for compliance. *Canadian Journal of Law and Technology* **17**, 276–305.

Wang D, Zhao J and Wang Y (2020) A survey on privacy protection of blockchain: the technology and application. *IEEE Access* **8**, 108766–108781.

Werbach K (2018) *The Blockchain and the New Architecture of Trust*. Cambridge: MIT Press.

Wirth C and Kolain M (2018) Privacy by blockchain design: a blockchain-enabled GDPR-compliant approach for handling personal data. *Reports of the European Society for Socially Embedded Technologies* **2**, published online at: https://dl.eusset.eu/bitstream/20.500.12015/3159/1/blockchain2018_03.pdf (accessed 30 August 2022).

Yeung K (2019) Regulation by blockchain: the emerging battle for supremacy between the code of law and code as law. *The Modern Law Review* **82**, 207–239.

Zaslowsky D (2021) *Block.one to Pay $27.5 Million to Settle Class Action Lawsuit Related to ICO – Blockchain*. Available at: https://blockchain.bakermckenzie.com/2021/06/17/block-one-to-pay-27-5-million-to-settle-class-action-lawsuit-related-to-ico/ (accessed 4 October 2021).

Zhao JL, Fan S and Yan J (2016) Overview of business innovations and research opportunities in blockchain and introduction to the special issue. *Financial Innovation* **2**, 1–7.

Cite this article: Baquero PM (2023). Layers of privacy in the blockchain: from technological solutionism to human-centred privacy-compliance technologies. *International Journal of Law in Context* **19**, 51–69. https://doi.org/10.1017/S1744552322000465