2024 6th Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS) | 979-8-3503-6784-3/24/$31.00 ©2024 IEEE | DOI: 10.1109/BRAINS63024.2024.10732409

On Addressing Governance Challenges in Blockchain Networks

Sokratis Vavilis
Inlecom Innovation
Athens, Greece
https://orcid.org/0000-0002-3104-3973

Harris Niavis
Inlecom Group
Brussels, Belgium
https://orcid.org/0000-0002-5941-9987

Lucía Recolons García-Mauriño
Verdia Legal, S.L.P.
Barcelona, Spain
lrecolons@verdialegal.com

***Abstract*—The governance of blockchain networks presents unique challenges in ensuring privacy and accountability in operational processes. This work examines current obstacles within existing governance structures and proposes directions towards the privacy-preserving governance of blockchain networks. We explore the complexities of data protection, smart contract accountability, and operational governance, highlighting the discrepancies between traditional governance models and the decentralized nature of blockchain ecosystems. To this end, we propose integrating legally binding smart contracts and Ricardian contracts, along with practical guidelines for blockchain administrators aiming to enable enhanced privacy, regulatory compliance, and efficient dispute resolution mechanisms.**

***Index Terms*—Blockchain, Governance, Privacy, GDPR**

I. Introduction

The proliferation of blockchain technology has introduced promises of decentralization, transparency, and immutable record-keeping across various sectors. As blockchain networks continue to evolve and expand their applications, the need for robust governance becomes increasingly evident [1]. However, amidst the potential benefits, significant challenges persist, particularly in ensuring data protection, orchestrating smart contract execution, and establishing accountability in operational governance within blockchain ecosystems [12].

Traditional governance models often struggle to adapt to the unique characteristics and complexities of blockchain networks [1]–[3]. The decentralized nature of these networks presents novel challenges for regulatory compliance, privacy, and accountability. Moreover, the autonomous execution of smart contracts [14] introduces additional complexity, raising concerns about legal enforceability, dispute resolution, and the protection of stakeholders' interests.

This work explores the current challenges faced by governance frameworks in blockchain networks, with a particular focus on addressing issues related to data protection, smart contract legal enforceability, and operational governance. We delve into the intricacies of these challenges, highlighting the gaps between existing governance mechanisms, governance standards and the unique demands of blockchain ecosystems.

To bridge these gaps, we propose guidelines towards a privacy-preserving governance framework for blockchain. Central to this framework are legally binding smart contracts and Ricardian contracts, which offer a promising approach ensuring privacy, regulatory compliance, and facilitating efficient dispute resolution within blockchain networks. Our aim is to facilitate the design of a comprehensive solution that integrates legal and technical mechanisms, seeking to contribute to the ongoing discourse on governance innovation in blockchain.

In the subsequent sections of this paper, we delve deeper into the conceptual underpinnings of our approach, elucidating its key components, implementation strategies, and potential implications for the future of governance in blockchain networks. The rest of the paper is organised as follows. Section II presents the related legal framework and regulations. Section III describes current challenges in blockchain governance, while Section IV introduces a governance framework and presents guidelines for regulatory compliance and legal accountability. Section V concludes and points out directions for future work.

II. Data Protection Regulations and GDPR

A key functionality of blockchain networks is storing and managing data in a decentralized manner. Thus, it is important to understand the impact of existing legislation governing the protection of data. One of the most prominent examples of such legislation is the General Data Protection Regulation (GDPR). GDPR aims to pose the legal framework under which organizations have to operate when handling Personal data.

*a) **Personal Data**:* The definition of personal data determines the GDPR's scope of application and is accordingly of paramount importance. The Regulation only applies to data that is considered 'personal' in nature. For this reason, it is first necessary to identify what is meant by personal data.

Article 4(1) of GDPR defines personal data as follows: *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*

In practice, to better clarify which pieces of information should be considered as personal data, thus governed by the GDPR, identifiability criteria should be properly defined.

*b) **The criteria of identifiability**:* According to Art. 29 WP [11], three different criteria ought to be considered to determine whether an individual is identifiable through data.

Singling out refers to the possibility of isolating some or all records that identify an individual in the dataset. An example would be a dataset containing medical information that enables the identification of a specific data subject, for example, through a combination of medical information and additional demographic factors [10].

Linkability denotes the risk generated where at least two data sets contain information about the same data subject. Whether, in such circumstances, an attacker can establish (e.g., by means of correlation analysis) that two records are assigned to the same group of individuals but cannot single out individuals in this group. Assessing linkability is challenging as it is hard to establish what other information capable of triggering identification through linkage is available to a controller now or in the future [10].

Inference has been defined as 'the possibility to deduce, with significant probability, the value of an attribute from the values of a set of other attributes. For example, where a dataset refers not to Angela Merkel but rather to a female German chancellor in the early 2000s, her identity would nonetheless be possible to reasonably infer.

Based on the above, if a piece of data satisfies any of the identifiability criteria, it should be deemed as Personal Data and handled according to GDPR.

III. Governance Aspects and Challenges in Blockchain Networks

Modern organizations need to address a plethora of issues to ensure their proper operation and management. For instance, issues related to membership, roles and responsibilities, accountability, decision-making procedures, and compliance with legislation. These aspects are commonly referred to as governance. In traditional organizations, governance is usually defined in a formal manner (e.g., documentation on procedures) and its enforcement is based primarily on their legally binding nature. Similarly, in blockchain networks, the related issues are addressed by blockchain governance [3]. However, due to the technology's decentralized nature, blockchain governance faces particular challenges that may hinder its effectiveness [2]. In this section, we discuss the blockchain governance challenges related to its operation, smart contracts, and compliance with the existing legal framework, particularly the one related to data protection.

A. Operational Governance challenges

By operational governance, we refer to all the generic governance matters that have to be resolved by an organization belonging to a blockchain network. Existing blockchain standards [5], [6] recognize the challenging nature of blockchain governance but focus on providing higher-level guiding principles rather than concrete directions. For instance, IEEE 2145-2023 [6] is normative only for terminology and non-normative in terms of design, governance models, and protocols.

1) Public and Permissionless: One of the most important aspects of governance is membership due to its direct link to other aspects, such as decision processes, roles, etc [3]. In public and permissionless blockchain networks, where membership is completely open, assigning roles to the members and enforcing procedures is challenging and mainly relies on the punctuality of each node and the mechanisms employed by the network [2], [3]. Similarly, assigning and monitoring responsibilities, including accountability, is equally challenging. The governance and operations of such networks typically rely on the alignment of the self-interest of the participants with the common good of the network. To this end, incentives have a pivotal role as they provide a motivational factor that influences members' behavior, effectively putting pressure on the members to comply with the rules. Such incentive mechanisms are usually integrated into the actual design of the network (e.g., consensus mechanism) and the implemented code. However, finding the right type of incentives is challenging and may affect the fairness of the effectiveness of the blockchain [3], [4]. The most typical incentive mechanism is awarding nodes that successfully add new blocks to the chain and punishing nodes (i.e., by losing part of their stake) when they fail to fulfill their responsibilities.

For decision-making in public and permissionless networks, two main governance models exist, namely off-chain and on-chain [2]–[5]. In the off-chain governance model, decisions are usually made informally through discussions, debates, and decision-making processes that occur outside of the blockchain. To this end, several supporting mechanisms can be employed, such as online platforms, fora, shared code repositories, etc. In such cases, developers, founders, and key figures of the network may have a significant impact on the off-chain governance, although this is not always the case. For instance, the Ethereum community implements an off-chain governance model, where any member of the network may submit an Ethereum Improvement Proposal (EIP) to propose changes to the network. Intuitively, the community will agree on beneficial EIPs, however, this is not always true, leading to the formation of hard forks.

Another key limitation of off-chain governance is the lack of an enforcement mechanism for the decisions made [2], [3]. On-chain governance model treats this issue by leveraging the unique features of blockchain technology to make decisions. Such an approach is commonly referred to as "the rule of code". In particular, smart contracts are employed to support governance processes and enforce decisions made. This makes them an ideal candidate for public blockchains, as all processes are automated and can be audited by any user. A typical example of on-chain governance can be found in Decentralized Autonomous Organizations (DAOs), which automate governance processes with smart contracts.

In practice, however on-chain governance of public permissionless networks can be problematic. Due to loose membership, this model although seemingly democratic, faces other challenges, such as low membership participation, manipulation of the voting process using Sybil attacks, or manipulation of the outcome by important nodes (e.g., nodes with comparatively high stake) [3], [4]. Lastly, we note that not every governance aspect can be easily implemented in code [1].

2) Private and Permissioned: Private and permissioned blockchain networks face fewer challenges compared to their public permissionless counterpart. Although incentivization can be employed, due to their better-defined membership, it is possible to properly define roles, responsibilities, and procedures and assign accountability [2], [3]. Therefore, their challenges are quite similar to the governance aspects of traditional IT or Cloud-based organizations. However, we would like to highlight that on a large scale, solving such issues can be challenging due to the high level of decentralization and the associated complexity of legal procedures.

In terms of decision-making in private and permissioned networks, the situation is similar to its counterpart. In particular, both off-chain and on-chain models are applicable, and their complexity can be reduced by leveraging the better definition of members and roles. Although this may lead to increased centralization and reduced democracy in the network, it has the benefit that the integrity of the decision-making process cannot be easily affected by members (e.g., Sybil Attacks) [2]. Lastly, we note that in practice on-chain governance model may not fully leverage the benefits of smart contracts, as they are not considered legally binding agreements.

B. Smart Contracts legal challenges

Albeit the many benefits of smart contracts, their legal status is considered an open issue. Generally, for smart contracts to be considered legally binding agreements (i.e., contracts), a minimum of criteria should be satisfied [1]. The applicable law and jurisdiction to which the parties submit a contract for the resolution of disputes must be identified. This is essential to determine the requirements that will govern all contracts. In this sense, Common Law tends to be more flexible when considering the legal validity and requires less regulation and more interpretation (in comparison to Civil Law).

Although the minimum contract elements vary in every legislation, we could identify the following [2]: *applicable jurisdiction, parties to the contract, the subject matter of the contract, consent, capacity of the parties, cause and form of the contract, and signatures*.

It is important to note that the signatory parties agree with the agreed conditions (consent), as well as that they are identifiable and legally entitled to sign these contracts. Moreover, consideration should be given not only to the legal capacity of the signing parties (e.g., age of majority of the persons) but also to the "cause" of a contract when determining the reason or object for which the contract is concluded. The "form" indicates the outward expression or manifestation of the contract. Depending on the jurisdiction, this form can be free (e.g., oral form), or imposed (usually in paper form). Lastly, contracts should include valid signatures. Currently, both the structure and content of existing smart contracts do not directly meet these criteria. Therefore, assigning legally binding properties to them is a challenge to be addressed.

[1]https://harris-sliwoski.com/blog/are-smart-contracts-legal-contracts

[2]Those elements are common in the Civil Law jurisdictions (e.g., Spain, France, and Italy).

C. Data Protection and GDPR challenges

Data protection regulations, such as the GDPR, have an impact on what is stored on-chain. A key challenge arises from the fundamental data subject rights defined in GDPR. More precisely, the right to be forgotten, which dictates the right of an individual to demand the erasure of their personal data, is deemed incompatible with the immutable nature of blockchain. Thus, personal data cannot be directly stored on-chain.

Currently, there is ample uncertainty as to when the line between personal and non-personal data is crossed in practice. The principle that should be used to determine whether data is personal or not is that of the reasonable likelihood of identification, which is enshrined in Recital 26 GDPR according to which identifiability criteria are set.

Next to that, Art. 29 WP leaned towards a zero-risk approach related to the likelihood of identifiability [10]. Transforming personal data in a manner that excludes singling out, linkability, and inference in a reasonable manner is difficult. This is confirmed by the WP's analysis of the most commonly used 'anonymisation' methods, which concluded that each of them leaves a residual risk of identification. It is crucial to note that the EU considers that pseudonymous data on a blockchain can, in principle, be related to an identified or identifiable natural person [13]. Thus, direct use of pseudonymisation of personal data in blockchain is non-compliant with the GDPR.

Even when personal data is not directly stored in the blockchain but is managed in a distributed manner using blockchain, data subject right has major practical implications on the governance of the network. For instance, the compliance with the right to be forgotten can only be given where the personal data in question is erased from all of the nodes that participate in the network, which is a challenging task.

IV. Towards a Privacy-Preserving Governance Framework for Blockchain

In this section, we discuss potential solutions to the already described challenges, paving the way towards a privacy-preserving governance framework for blockchain.

A. Achieving GDPR Compliance

To address the right to be forgotten, several technical solutions have been proposed. For instance, a solution could be the storage of encrypted personal data on-chain using public key cryptography. In this case, the destruction of the private key (stored off-chain), will render the encrypted data inaccessible. This is indeed the solution that has been put forward by the French data protection authority CNIL in its guidance on blockchains and the GDPR [9].

Another solution is storing personal data off-chain, and merely linking them to the blockchain through a cryptographic hash. Such a process is considered to have several advantages from a data protection perspective [13], since it makes it easier to comply with GDPR requirements, without changing the nature of personal data. If data needs to be erased, the records in the database can be deleted, leaving the immutable hash

on the blockchain referencing non-existent data. Data subject rights can be enforced via smart contracts, as we will see in Section IV-C.

B. Legally binding Contracts

As mentioned in Section III-B, even if smart contracts include the essential elements of a legal agreement (e.g., as constant variables), they cannot be considered legally binding in all cases. Since they are digitally signed, the applied jurisdiction should accept the legality of digital signatures. When digital signatures are not recognised by the authorities, such a challenge can be addressed by Ricardian Contracts.

A Ricardian Contract can be defined as a document that is a) a contract offered by an issuer to holders, b) for a valuable right held by holders, and managed by the issuer, c) easily readable by people, d) readable by computer programs, e) digitally signed, f) carries the keys and server information, and g) allied with a unique and secure identifier [7], [8].

Essentially, the concept of Ricardian contracts creates a bridge between the legal and digital realms, by combining a human and machine-readable legal document and machine code. We note that the human-readable part of a Ricardian contract, can be used and be legally recognized as a regular (i.e., paper-based) contract even in jurisdictions that do not recognize digital signatures. To further facilitate enforeability, we propose that participants when joining a blockchain network should provide their acceptance of the legal validity of the smart contracts employed by the network in an initial agreement. All subsequent Ricardian contracts of the network will fall under the initial agreement signed by the participants.

C. Operational governance

We argue that adopting on-chain governance models reinforced with legally binding (Ricardian) smart contracts will have a catalytic role in blockchain operational governance.

To this end, we propose the adoption of Ricardian smart contracts which will document agreements in a human-readable and legally binding manner and will implement its content in machine code. In more detail, the constitutional agreements of a blockchain network, different procedures and any other potential agreement will be documented on paper (albeit in digital format) as proper legal documents. Such documents may include any needed detail, clauses to be respected and steps to be followed by the participants. All these details will then be transformed into smart contract code running on the blockchain, to automatically monitor, follow, and enforce the implemented clauses. To overcome the technical limitations of smart contracts, we propose the use of dedicated oracles for implementing the agreement clauses that require interaction with the environment outside of a blockchain network. For instance, to enforce the right to be forgotten, an oracle should be created that will erase personal data stored off-chain upon request, and will provide sufficient evidence to the related Ricardian smart contract.

We note that, in *public permissionless* blockchains some advantages of our approach might not be fully leveraged due to the loose membership of the network. In that case, obscure participants' identities might affect the legal enforcement of accountability. However, this is a challenge directly related to any organization with anonymous members. Finally, in the case of *permissioned* blockchain networks, the benefits of the proposed approach are straightforward.

V. Conclusions

In this work, we presented the key blockchain governance challenges, with a particular focus on its compliance with data protection regulations. Following an interdisciplinary approach, we discussed potential solutions to these challenges, moving towards creating a privacy-preserving governance framework. While a practical implementation is still needed, we made a significant step forward in reconciling the decentralized nature of blockchain with the demands of effective governance. As a future step, we intend to apply our approach in the context of the InEExS project.

Acknowledgment

The current paper was based on the research conducted within the framework of the LIFE project "InEExS— Innovative Energy (Efficiency) Service Models for Sector Integration via Blockchain" https://ieecp.org/projects/ineexs/ (Co-funded by the European Union under project ID101077033). The contents of the paper are the sole responsibility of its authors and do not necessarily reflect the views of the EC.

References

[1] Beck, Roman et al. "Governance in the Blockchain Economy: A Framework and Research Agenda," Journal of the Association for Information Systems, (2018).
[2] Liu, Yue, et al. "A systematic literature review on blockchain governance." Journal of Systems and Software (2023).
[3] Rikken, Olivier, Marijn Janssen, and Zenlin Kwee. "Governance challenges of blockchain and decentralized autonomous organizations." Information Polity (2019).
[4] Pelt, Rowan van, et al. "Defining blockchain governance: A framework for analysis and comparison." Information Systems Management (2021).
[5] International Organization for Standardization. (2022). Blockchain and distributed ledger technologies - Guidelines for governance (ISO Standard No. 23635:2022).
[6] "IEEE Trial-Use Recommended Practice for Framework and Definitions for Blockchain Governance," in IEEE Std 2145-2023, 2024
[7] Grigg, Ian (2004). "The Ricardian contract". First IEEE International Workshop on Electronic Contracting, 2004. IEEE.
[8] Hazard, James and Haapio, Helena, Wise Contracts: Smart Contracts that Work for People and Machines, Trends and Communities of Legal Informatics. Proceedings of the 20th International Legal Informatics Symposium IRIS 2017
[9] Commission Nationale Informatique & Libertés (2018). "Blockchain: quelles solutions pour un usage responsable en présence de données personnelles?" . //www.cnil.fr/sites/cnil/files/atoms/files/la_blockchain.pdf
[10] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques (0829/14/EN WP 216)
[11] Article 29 Working Party, Opinion 04/2007 on the concept of personal data (01248/07/EN WP 136)
[12] J. Al-Jaroodi and N. Mohamed, "Blockchain in Industries: A Survey," in IEEE Access 2019
[13] European Parliamentary Research Service. "Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?" July 2019
[14] Wood, G., "Ethereum: A secure decentralized generalized transaction ledger." 2023