Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 198 (2022) 662–669

Procedia Computer Science

www.elsevier.com/locate/procedia

The 8h International Workshop on Privacy and Security in HealthCare (PSCare 2021)
November 1-4, 2021, Leuven, Belgium

Blockchain-based governance models for COVID-19 digital health certificates: A legal, technical, ethical and security requirements analysis

Mark Foy*, Dolores Martyn,[a] Debra Daly,[a] Aoife Byrne,[a] Chinwe Aguneche,[a] and Rob Brennan[a,b]

[a]*School of Computing Dublin City University, Dublin, D09 Y074, Ireland*
[b]*ADAPT Centre, Dublin City University, Dublin, D09 7074, Ireland*

Abstract

This paper analyses the requirements of a blockchain-based data governance model for COVID-19 digital health certificates. Recognizing a gap in the existing literature, this paper aims to answer the research question "To what extent does a blockchain-based governance model for COVID-19 digital health certificates in the EU meet the relevant legal, technical, ethical and security requirements?" This paper identifies the required standards and develops a novel framework to determine the viability of blockchain as a governance model. The results of our evaluation indicate that while a private permissioned blockchain can meet the requirements to some degree, the governance element is key to legal compliance; legal risks and ethical implications remain unresolved with the use of blockchain. The paper also found that this model comes with the loss of the main advantages of blockchain – decentralization and anonymity. This evaluation framework may be used in other contexts and for assessing other technologies.

Keywords: blockchain; governance; GDPR; legal analysis; health certificate; COVID-19

*Corresponding author.
Email address: mark.foy4@mail.dcu.ie.

10.1016/j.procs.2021.12.303

1. Introduction

Within the existing literature, papers both advocate and critique a blockchain-based governance model. Notably, Halpin describes how identity systems based on globally unique identifiers are "by nature against privacy and putting them on a blockchain does not change this fundamental dichotomy" [3]. Many enthusiasts, however, promote the blockchain as a more efficient, decentralized and consensus-driven public repository, which can have several applications in order to make citizens less dependent on governments, yet within a society that is ultimately founded upon the State authority [4]. For the purposes of this research, we define a "Blockchain Governance Model" as a data governance model which establishes decision domains and accountability for decision making while using blockchain technology. This is a development of Khatri & Brown's data governance definition [5].

To the best of our knowledge, there is yet no multifactor analysis of whether a blockchain-based model for COVID-19 health certificates would be viable in terms of legal, security and technical requirements–all of which are foundations for creating an effective governance model. In fact, the concept of data governance is largely absent from research papers on this topic. The rest of this paper is structured as follows: section 2 surveys the background literature, section 3 identities the requirements for evaluation of blockchain-based digital health certificates, section 4 describes our evaluation framework design, section 5 discusses the evaluation results and section 6 provides conclusions.

2. Background

The research method adopted was based on qualitative and comparative research. This was implemented through looking at themes of blockchain and immunity passports in the literature. We set out a general research question, selected relevant material, collected the relevant literature, conceptualized and theorized our work and then wrote up our findings following the qualitative method requirements. The qualitative research tools used throughout our research were record keeping and observation of literature related to our research area. In particular, the use of Google Scholar allowed us to gather reliable information from one location, along with using our institution's digital library databases. The following themes were identified: Legal implications of health certificates, blockchain, GDPR and heath certificates, security issues with blockchain governance, cross-border movement. Each is discussed below.

2.1. Legal implications of blockchain-based health certificates

Many legal implications that arise regarding COVID-19 health certificates are yet to be fully addressed. Issues identified in the literature so far include inequality, health-status based discrimination, the sharing of medical data and concerns with respect to the GDPR [6], and human rights issues. The unanimity amongst the literature is that health certificates would "impose an artificial restriction on who can and cannot participate in social, civic, and economic activities and might create a perverse incentive for individuals to seek out infection, especially people who are unable to afford a period of workforce exclusion, compounding existing gender, race, ethnicity, and national inequities" [7].

A suspension of human rights must be data-driven and evidence based [8], and there must be some other previously standing framework that can provide "sufficiently clear and precise rules". Currently there is no known specific or general framework which can provide sufficient clarity on how blockchain-enabled immunity credentials would be either governed or processed.

One concern in relation to human rights is that "The most concrete immunity passport proposal dangerously puts the hash of personal data on the blockchain. Even the use of blockchain technology by specifying resolution of an on-chain mapping of an identifier to a key in public-permissioned blockchain systems like Sovrin ends up being a redirect to centralized servers, undermining a claim of the blockchain promoting decentralization" [3].

Powers illustrates that since blockchain is built for data integration and not for the purpose of privacy, there are possible attacks on the personal information being stored within the framework [9]. Halpin also notes, "As the use of blockchain technology does not seem necessary for the goals of the immunity passports and likely hinders rather

than helps privacy, immunity passports – and more widely both W3C DIDs and VCs – use blockchain for blockchain's sake" [3].

2.2. Blockchain and the GDPR

There is a general consensus that blockchain falls within the scope of the GDPR when personal data is processed, as the data (public keys and transactional data) is pseudonymized, not anonymized [10]. There appears to be irreconcilable tensions between blockchain and the GDPR as blockchain technology's distributed peer-to-peer network architecture often places it at odds with the GDPR's traditional notion of centralized controller-based data processing [11]. Issues of conflict include identifying the data controller and processor, territorial scope, principles including accountability, purpose limitation, storage limitation and data minimization; and data rights such as access, right to rectification and right to erasure [12].

The European Parliament's guidance on blockchain and the GDPR records how it is impossible to state that blockchains are either completely compliant or noncompliant with the GDPR. It notes that numerous important points of tension have to be highlighted but "ultimately each concrete use case needs to be examined on the basis of a detailed case-by-case analysis" [13].

The legal literature explores numerous ways a blockchain model could be more compliant with the GDPR, for example using a permissioned blockchain. In these cases, it may be possible to identify a central intermediary that can qualify as the data controller, such as the system's operator [14]. Off-chain data storage is seen as a possible workaround to enable the GDPR's right to rectification and right to erasure [6]. It may be possible to design a blockchain platform so that any personal data is not stored on the chain, but is stored in encrypted form in a separate, off-chain database [15]. It is important to note that whereas it will often be possible to store transactional data off-chain, this is not the case for public keys [13].

2.3. Security issues with blockchain governance of health certificates

Blockchain governance has become one of the most frequently discussed methods for securing data storage and transfer through decentralized, trust-less, peer-to-peer systems [16]. Blockchain technology can provide security guarantees that resolve many traditional challenges in addition to providing a fully distributed, secure, consensus solution.

Although security may be a selling point of blockchain, it is important to acknowledge the security issues that are present. Several authors namely Oksiiuk and Dmyrieva [11], Zhang and Xue [17], Dai, Shi, Meng, Wei and Ye [18], and Yaga, Mell, Roby and Scarfone [14] have discussed security issues with blockchain. These include 51% attacks, phishing and social engineering, and stolen cryptocurrencies. Frankenfield [18] characterizes 51% attacks as an attack on a blockchain by a group of miners controlling more than 50% of the network's mining hash rate or computer power. Attackers would be able to prevent new transactions from gaining confirmations, allowing them to halt payments between some or all users. Oksiiuk and Dmyrieva [11] discuss phishing and social engineering as some of the most widespread attacks in cryptocurrency today. In these attacks, malicious parties use a variety of tricks to dupe unsuspecting victims into sending over their private keys or login information. They also explored the issue of stolen cryptocurrencies and discussed how insecure or negligent storage of a blockchain privacy key can lead to theft or loss [11].

Security analysis and risk assessment should be used in the designing of the infrastructure to assure sufficient levels of protection against forgery of certificates or reuse of valid certificates issued for other persons [19]. Recent eHealth Network Guidelines on verifiable vaccination certificates establish that a trust framework, which includes a digital infrastructure, is needed for establishing the authenticity and validity of certificates presented by certificate holders [19].

2.4. Technical concerns with blockchain governance

Two practical concerns when considering the use of a public blockchain are the computational and environmental cost. The average blockchain transaction can take 200kWh of energy to verify, enough to power a house for a month

[26]. This is due to the Proof of Work (PoW) which has been a point of analysis and critique [20] [21]. The transactions are also slow with the average confirmation time being 10 minutes, and the potential to be longer [22]. Proof of stakes have been proposed as a quicker and lower-energy alternative to PoW, but they too have disadvantages [23].

A private blockchain has the advantages of having a low PoW and quick transaction approval of the order of milliseconds rather than minutes [24]. However, private blockchains are centralized and have identified users, sacrificing two of the main benefits of a public blockchain – decentralization and anonymity.

Beck, Muller-Bloch, and King [25] have put forward a framework by which the governance of a blockchain-based organization can be analysed where the traditional notions of accountability, incentives and decision rights are altered in a blockchain-based system.

3. Requirements

From the previous section we see that legal, security and technical considerations must be evaluated for blockchain as a governance model for COVID-19 health certificates. Any potential data governance model also needs to meet adequate ethical standards. Table 1 below lists the factors which must be considered when evaluating whether a technology is a good basis for health certificates and the data governance aims.

Table 1. Areas of Analysis for Blockchain-based Health Certificates and Data Governance Aims.

Analysis Facet	Data Governance Aims
Ethical	• Prevents discrimination
	• Respects Privacy
	• Establishes Trust
Technical	• Scalability
	• Low Cost – Financial and Temporal
	• Available technology
	• Low Energy Usage
Security	• Protects Personal Data
	• Tamper-resistant
	• Ensures Data Integrity
Legal	• GDPR Compliant
	• Cross Jurisdiction Compatibility
	• Upholds Human Rights

4. Evaluation Framework Design

To assess if, or to what extent, the use of blockchain technology could meet these health certificate requirements we created an evaluation framework made up of individual assessments of blockchain's compliance with our designated ethical, legal, technical and security requirements. We were then able to combine these into an overall analysis of how viable different types of blockchain are for this purpose and identify risks that remain. Deploying an appropriate blockchain technology is insufficient for strong data governance, as this is also dependent on the implementation of an effective data governance model.

To evaluate how compliant a proposed blockchain model for health certificates is with ethical standards we applied the Ethics Canvas [26]. This helped to highlight gaps in system knowledge, make us think about how this application will affect others and highlight questions that need to be asked before the implementation of COVID-19 health certificates.

For our legal analysis we examined blockchain's compliance with the GDPR, cross border movement and human rights. To determine if various blockchain models meet GDPR requirements we developed our own evaluation

framework (Table 2). This assesses if the various GDPR principles and data subject rights can be met when using a private or consortium & permissioned blockchain, a public permissioned blockchain, and a public & permissionless blockchain.

Table 2. GDPR and blockchain types overview.

Blockchain Type GDPR Requirements	Private Permissioned	Public Permissionless	Public Permissioned
Accountability (Data Controller)	Yes	No	Yes
Data Minimisation	Yes	No	No
Appropriate Security Measures	Yes	Yes	Yes
Accuracy of Data	Less control (Data will be input by various actors)	No	Less control (Data will be input by various actors)
Storage Limitation	Possibly (Off chain)	No	Possibly (Off chain)
Right to Rectification/Erasure	Possibly (Off chain)	No	Possibly (Off chain)
Right to Access Data	Possibly (Off chain)	No	Possibly (Off chain)

From a technical point of view, we considered the financial cost, temporal cost, energy usage, scalability and availability when evaluating whether blockchain is a good basis for vaccine passports. Furthermore, the chosen technology should facilitate all the security, legal and governance requirements. For this analysis we adapt and use the flowchart produced by the US Department of Homeland Security Science and Technology Directorate for the purpose of determining if an initiative requires blockchain [14].

The conclusion of this analysis was that a private permissioned blockchain was the most suitable to satisfy the ethical, legal, technical requirements for health certificates. This blockchain type alone is not enough to reach compliance levels, however, without a strong data governance model. We identified Khatri and Brown's data governance framework as a suitable governance model that assessed decision domains key to our project; data principles, data quality, metadata, data access and data lifecycle [27].

We then applied Khatri & Brown's locus of accountability matrix [27] to assess how many of these decision domains are centralized and how many are decentralized when using a blockchain for the purpose of COVID-19 health certificates (Fig 2). This allowed us to assess if the blockchain model that meets our designated ethical, legal, technical and security requirements has a mostly centralized or decentralized decision making process.

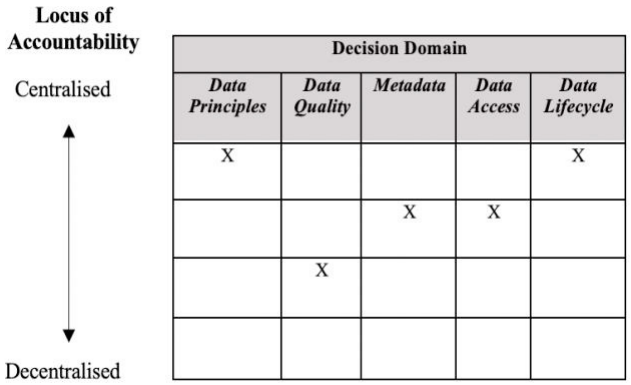

Fig. 1. Locus of accountability scores for a private permissioned blockchain.

5. Discussion

5.1. Legal

Table 2 shows a sample of the GDPR and blockchain analysis and is representative of the overall conclusion that a private, permissioned blockchain is needed in this instance to meet GDPR requirements, particularly the obligations to identify a data controller and limit personal data stored to what is strictly necessary. Other requirements such as the right to rectification or right to erasure can be met with extensions, such as storing personal data off the chain. It must be noted that if the legal basis is not consent and is instead processing in the public health interest then derogations apply [6]. For example, there may be no need to comply with the right to be forgotten [6].

A private permissioned blockchain network alone, however, is not enough to meet GDPR requirements and issues remain. Due to the scale of this type of project, the processing of special categories health data (and potentially biometric data), and the use of blockchain a Data Protection Impact Assessment is crucial to identify risks which may be amplified due to the permanent immutable nature of blockchain. An effective data governance model is also necessary to mitigate risks, for example blockchain's selling point is its verifiable nature but this doesn't guarantee the accuracy of data input on the chain; efficient governance is essential to reaching these goals.

5.2. Technical

Two types of blockchain were considered for technical analysis, permissionless and permissioned. In permissionless blockchain, like bitcoin, anyone can join and can approve transactions anonymously. In a permissioned blockchain, access and approval to the blockchain is governed by a central authority. The time needed to approve a transaction is about 10 minutes for a permissionless blockchain but on the order of μseconds for a permissioned blockchain.

Energy usage is very high for a permissionless blockchain. An average transaction takes 200kWh, which is enough to power a house for a whole month. A permissionless blockchain is decentralized and anonymous, whereas a permissioned blockchain is centralized and everyone involved is identified. Scaling up presents some difficulties for a permissioned blockchain. For example, an increase in blockchain size slows down the propagation of the updated blockchain across the network; and increasing the rate of transactions decreases security. Overall, a permissioned blockchain is a more practical technical solution than a permissionless blockchain as waiting 10 minutes for your immunity status to be validated or using so much energy would not be feasible.

5.3. Security

Blockchain can provide many security guarantees solving traditional challenges around security and privacy. Blockchain is created and maintained using a peer-to-peer overlay network and secured through intelligent and decentralized utilization of cryptography with crowd computing [17]. The blockchain model meets these security demands. Cryptographic techniques are used to secure each block on the chain, reinforcing the integrity and security of transactions. The integrity of data content stored on the blockchain is guaranteed as retrospective alteration of transaction records is impossible once a block has been successfully created. Basic security properties of blockchain ensure the restriction of access to data which include the use of public and private key access. Public and private keys are used to digitally sign and transact in a secure manner within the blockchain system and are an extremely important aspect of the technology. The private keys are used by individuals to decrypt data and are the sole responsibility of the user. This however may align with the question of whether blockchain is an overkill; if a user loses a private key, then any digital asset, or in our case an immunity certificate, is lost. It is computationally infeasible to regenerate the same private key [14]. This might be a big ask for the general public and one may question whether this level of security is necessary. By applying the US Department of Homeland Security Science and Technology Directorate's 'Do we need blockchain?' flowchart we found although there may still be a useful blockchain use case, there are some stages that indicate that an encrypted database would be sufficient for the storage of health certificates.

5.4. Ethical

When applying the Ethics Canvas, we found that the individuals who would be using the private permissioned blockchain governance model would be any citizen who wishes to obtain a COVID-19 health certificate, affecting all members of society. It would allow for those who do not have a risk of reinfection to see friends, family-members, and co-workers in a face-to-face encounter and without COVID-19 guidelines applying. Nonetheless, there are ethical issues with respect to inequality, health-status based discrimination, the sharing of medical data and GDPR.

For example, a vaccination may not be possible for some people due to health reasons, and it needs to be considered how their movement could be enhanced. A potential service failure in the case of a private permissioned blockchain is the possible attacks on personal information being stored within the framework, since blockchain is built for data integration and not for the purpose of privacy. The pre-eminent ethical impacts are the insurance of privacy and the protection of individuals regarding their personal data. In order to address this, we have exhausted the legal, technical and security requirements which arise with the implementation of health certificates using a private permissioned blockchain based governance model. Questions remain regarding the human rights implications of COVID-19 health certs, as well as scientific questions on immunity and the spread of the virus which raise red flags over the use of a permanent infrastructure such as blockchain.

5.5. Governance

The Khatri & Brown Locus of Accountability matrix shows the data governance decision domains on a scale ranging from centralized to decentralized; we found many of these aspects are centralized in a private permissioned blockchain. This high degree of centralized decision-making raises the question of whether blockchain is necessary at all. Using a private, permissioned blockchain comes at the loss of its two main selling points – decentralization and anonymity.

6. Conclusion

To conclude, our evaluation framework indicates that while it may be possible for a private permissioned blockchain-based COVID-19 health certificate to meet necessary legal, technical and security requirements to some extent, this comes at the loss of the main advantages of blockchain - decentralization and anonymity. Considering this along with the remaining legal risks and ethical implications, the use of blockchain may be overkill, offering a permanent solution to what is intended to be a temporary measure to exit the COVID-19 pandemic.

In previous work blockchain has been suggested as a solution without an explanation of how it would work and why it would be suitable. Our work has filled a gap in the existing literature by bringing together a comprehensive analysis of how blockchain can comply with the legal, security and technical requirements of COVID-19 health certificates. Our reusable evaluation framework for assessing the GDPR requirements against the different types of blockchains is nonetheless applicable in other contexts and for other technologies. We have also highlighted the importance of data governance in implementing this type of health certificate.

There were some limitations to our research, one such limitation being the lack of existing literature on cross-border movement for those in possession of a COVID-19 health certificate. This is a gap we intended to fill but were unable to, and perhaps this might be an area for future research going forward.

Acknowledgements

This research has received funding from the ADAPT Centre for Digital Content Technology, funded under the SFI Research Centres Programme (Grant 13/RC/2106_P2), co-funded by the European Regional Development Fund. For the purpose of Open Access, the author has applied a CC BY public copyright licence to any Author Accepted Manuscript version arising from this submission.

References

[1]. Enrique Dans, "Vaccination Passports Are The Only Way We Can Return To Normality," Forbes, 18 January 2021. [Online]. Available: https://www.forbes.com/sites/enriquedans/2021/01/18/vaccination-passports-are-the-only-way-we-can-return-to-normality/?sh=4461861043c7. [Accessed 16 April 2021].

[2]. Louisa Wright, "COVID-19: WHO races to develop vaccination card," DW, [Online]. Available: https://www.dw.com/en/covid-19-who-races-to-develop-vaccination-card/a-56352930. [Accessed 16 April 2021].

[3]. Harry Halpin, "A Critique of Immunity Passports and W3C Decentralized Identifiers," Lecture Notes in Computer Science, vol. 12529, 2020.

[4]. Marcella Atzori, "Blockchain Technology and Decentralized Governance: Is the State Still Necessary?," Journal of Governance and Regulation, vol. 6, no. 1, pp. 45-62, 2016.

[5]. Vijay Khatri and Carol V. Brown, "Designing Data Governance," Communications of the ACM, vol. 53, no. 1, pp. 148-152, 2010.

[6]. General Data Protection Regulation.

[7]. Alexandra L Phelan, "COVID-19 immunity passports and vaccination certificates: scientific, equitable and legal challenges," The Lancet, vol. 395, no. 10237, pp. 1595-1598, 2020.

[8]. Elizabeth M. Renieris, "The Dangers of Blockchain-Enabled "Immunity Passports" for COVID-19," Berkman Klein Center for Internet & Society at Harvard University, 18 May 2020. [Online]. Available: https://medium.com/berkman-klein-center/the-dangers-of-blockchain-enabled-immunity-passports-for-covid-19-5ff84cacb290.[Accessed 16 April 2021].

[9]. Benjamin Powers, "Blockchain-Based Immunity Passports Don't Resolve Core Issues," Coindesk, 7 December 2020. [Online]. Available: https://www.coindesk.com/blockchain-immunity-passports-core-privacy-issues. [Accessed 16 April 2021].

[10]. Michéle Finck, "Blockchains and Data Protection in the European Union," Lexxion, vol. 4, no. 1, pp. 17-35, 2018.

[11]. Oleksandr Oksiiuk and Iryna Dmyrieva, "Security and privacy issues of blockchain technology," IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), 2020.

[12]. Diogo Duarte, "An introduction to Blockchain technology from a legal perspective and its tensions with the GDPR," Academia, 2019.

[13]. Panel for the Future of Science and Technology, "Blockchain and the General Data Protection Regulation - Can distributed ledgers be square with European data protection law?," European Parliamentary Research Service (EPRS), 2019.

[14]. Dylan Yaga, Peter Mell, Nik Roby and Karen Scarfone, "Blockchain Technology Overview," National Institute of Standards and Technology 8202, 2018.

[15]. Jean Beacon et al., "Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers," Journal of Law & Technology, vol. 25, no. 1, 2018.

[16]. Paul Taylor et al., "A systematic literature review of blockchain technology," Digital Communications and Networks, 2019.

[17]. Rui Zhang and Riu Xue, "Security and Privacy on Blockchain," ACM Computing Surveys, vol. 1, no. 51, 2019.

[18]. Jake Frankenfield, "Investopedia," Investopedia, May 2019. [Online]. Available: https://www.investopedia.com/terms/1/51-attack.asp. [Accessed 2016 April 2021].

[19]. eHealth Network, "Guidelines on verifiable vaccination certificates - based interoperability elements," European Parliament , 2021.

[20]. Yue Hao et al., "Performance Analysis of Consensus Algorithm in Private Blockchain," IEEE Intelligent Vehicles Symposium (IV), pp. 280-285, 2018.

[21]. Marko Vukolic, "The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication," Springer, 2016.

[22]. Blockchain.com, "Blockchain Charts," Blockchain.com, [Online]. Available: https://www.blockchain.com/charts. [Accessed 16 April 2021].

[23]. Evangelos Deirmentzoglou, Georgios Papakyriakopoulos, Constantinos Patsakis, "A Survey on Long-Range Attacks for Proof of Stake Protocols," IEEE Access, vol. 7, pp. 28712-28725, 2019.

[24]. Fran Casino, Thomas K. Dasaklis, Constantinos Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," Telematics and Informatics, vol. 36, no. 0736-5853, pp. 55-81, 2019.

[25]. Roman Beck, Christoph Muller-Bloch, John Leslie King, "Governance in the Blockchain Economy: A Framework and Research Agenda," Journal of the Association for Information Systems, vol. 19, no. 10, 2018.

[26]. The ADAPT Centre for Digital Content Technology, "Online Ethics Canvas," [Online]. Available: https://www.ethicscanvas.org/. [Accessed 16 April 2021].

[27]. Vijay Khatri and Carol V. Brown, "Designing Data Governance," Communications of the ACM, vol. 53, no. 1, pp. 148-152, 2010.