The 10h IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT'2019
5-7 June, 2019, Leeds, United Kingdom

Blockchain Secured Electronic Health Records: Patient Rights, Privacy and Cybersecurity

Akarca D[1,3]* and Xiu PY[2,3]*, Ebbitt D[3], Mustafa B[3], Al-Ramadhani H[4], Albeyatti A[3]
[1]Faculty of Medicine, University of Southampton, Southampton, UK
[2] Leeds Teaching Hospitals NHS Trust, Leeds, UK
[3]Medicalchain.com Ltd, London, UK, {danyal, philip, dave, bara, abdullah}@medicalchain.com
[4]University of Manchester, hasan.al-ramadhani@student.manchester.ac.uk
*authors take responsibility for joint first authorship

Abstract—**There have been significant efforts in the UK to embrace health technology to improve provisions of care. Yet, healthcare offers unique challenges to innovation, particularly with regard to data siloing. Blockchain is a shared distributed ledger technology that decentralises information storage with the potential to improve health outcomes by concurrently optimising data sharing practices and data privacy. In this paper, we explore how blockchain technology may facilitate the handling of health data in the context of regulatory frameworks, patient rights, cybersecurity and provider-centric perspectives. This is essential if this developing technology is to be considered for implementation at scale.**

Keywords—Blockchain; Distributed ledger technology; Healthcare technology; Health informatics; Clinical trials, Electronic health records; Interoperability; Data exchange.

I. Introduction

In recent years, there have been significant concerted efforts by the UK government to embrace health technology to improve delivery and quality of care [1]. These efforts are in parallel to formal targets aiming to digitise health records by 2020 completely [2]. While successful in other industries, healthcare offers unique challenges to digital innovation. The scope of health data is highly complex; it is distributed across geographical space and requires specialist interpretation. From the perspective of a patient, their health information is fragmented across many siloed institutions. Altogether, this leaves health IT implementers in a challenging position, as digitising health data alone does not itself remove interoperability problems or lead to more effective utilisation of data by patients [3].

The greater awareness of these issues occurs at the same time as breakthroughs within the realm of decentralised computing, particularly within financial ledgers, through the invention of blockchain [4]. Blockchain offers an alternative model of record keeping to traditional databases that are resistant to data modification by operating in a decentralised fashion. Blockchain has attracted the interest of numerous upcoming electronic health record (EHR) software vendors [5, 6] who propose that the above data silo issues may be mitigated by using distributed ledgers. In Estonia, blockchain has already been implemented to secure healthcare data integrity for its entire population of 1.3 million citizens [7].

Healthcare data is valuable and is becoming increasingly ubiquitous, with estimates suggesting that medical knowledge doubles every 73 days [8]. Efforts to secure health data integrity while simultaneously providing patients with full access to their record should, therefore, be a priority. This is a core aspect of significant regulatory frameworks relevant to this area, in both the US and EU, that we explore in this paper. Indeed, the most significant advantage of a blockchain approach for maintaining distributed ledgers is arguably its security and ability for users to have ownership of their information. This is very important in the context of recent worrying trends of data breaches within large hospital institutions [9] alongside a growing movement of individuals rightly wanting transparency with regards to the dealings of their data.

This short piece puts forward a vision on how distributed healthcare records secured by blockchain technology may be understood in relation to patient rights, privacy and cybersecurity.

II. An Interoperable EHR Ecosystem Secured By Blockchain

Unlike traditional centralised databases, data held on a blockchain is distributed across multiple servers so that each has a simultaneous ledger of all transactions. Lists of data, termed *blocks*, are linked chronologically by cryptographic hashes (a digital signature) in an encrypted linear *chain*. The subsequent *blockchain* entails a complete history of prior transactions rendering it hack-resistant due to no single point of failure (a function of the network's distribution) alongside little to no economic incentive to tamper [4]. This provides an auditable record unalterable by a single party once the network collectively has confirmed block validity. Further blockchain experimental developments are underway, where a proportion of transactional information is kept off-chain for specific

978-1-7281-1733-1/19/$31.00 ©2019 IEEE

purposes, and this is later addressed. However, in general, blockchain entails the following fundamental features:

- A Peer to Peer (P2P) network that connects nodes (participants in the network) and propagates blocks of verified transactions.
- Transactions representing state transitions or information held on-chain.
- Consensus rules governing what constitutes a valid state transition.
- A consensus algorithm that decentralises control over the blockchain and ensures participants cooperate in the enforcement of the consensus rules.
- A state machine that processes transactions according to established consensus rules.
- Economic security through a game-theoretically sound incentivisation scheme (*proof of work* in the case of bitcoin) that economically secures the state machine (this is less relevant to non-public blockchains, which are discussed later).
- Data structures in a chain of cryptographically secured blocks, acting as an immutable reference of all confirmed state transitions.
- Software clients that typically combine all these above components.

These components provide the backbone of any blockchain system, including the most well renowned public blockchains *bitcoin* and *ethereum*. There are a range of advantages and disadvantages of a blockchain-based approach to record-keeping relative to traditional databases.

Importantly, there is a considerable variety of blockchain types with different operational properties. In some sense, many blockchain projects would be better understood if described by their characteristics rather than blockchain. Although there is not yet a universally accepted classification system, blockchains can be broadly distinguished as being public, private or hybrid.

Designs vary considerably depending upon the use-case in question. This variability is essential for this technology to be applied to the access of healthcare data, as an open public blockchain is not appropriate for handling sensitive health information. As in the case of Estonia, health information is secured by a blockchain quite dissimilar to the most well-known open blockchains.

In the UK, customised hybrid blockchain solutions have started to garner considerable interest by healthcare organisations whom for years have had significant issues with established EHR vendors. These vendors have provided strong in-system data consistency; however, have had little incentive to facilitate inter-vendor operability. As a result, there has been extremely slow progress of innovation in this area to the dismay of healthcare professionals and patients [3]. Moreover, healthcare organisations have found increasing vendor lock-in due to contractual and technical reliance. To counter these problems, open projects including openEHR [10] and FHIR [11] aim to facilitate the generation of openly adopted EHR standards and protocols to facilitate data exchange between vendors.

In summary, while centralised databases provide flexible operations within a siloed locality, upcoming interoperability standards may improve how these silos may communicate with each other more effectively. Blockchains may mitigate deeper issues relating to health-data security, auditability and user ownership. Similar to Estonia, we can be hopeful to incorporate a layer of blockchain security on top of existing infrastructures [12]. This may produce a more dynamic and flexible EHR ecosystem allowing for our long-term technological goals, from AI to genomics integration into routine care [1], to be better achieved. We now consider how this can be understood within regulatory frameworks.

TABLE I. Key Differences Between The Traditional Database And Blockchain Models [13]

	Traditional database		**Blockchain**	
Advantages	Stability	1. Large amounts of data quickly handleable; 2. Updates handled by a central planner who manages the whole system	Security	1. No single point of failure; 2. Decentralised information storage; 3. Decreased incentivisation for system attack
	Customisability	Easily alterable dependent on organisational requirements	Immutability	Once confirmed by the P2P network, blocks cannot be altered
	Transaction speed and volume	A high volume of transaction processing	Transparency	Transactional information is stored on every node of the P2P network (dependent upon off-chain features)
Disadvantages	Administrator use of information	1. No guarantee of the correct use of information; 2. Data utilisation may not reside with those who provide it; 3. Administrator privileges may always be changing.	Scalability	1. High volume on-chain transactions provide difficulty due to block size constraints; 2. Slow transaction rates can constrain uses
	Single point of failure	Single hacking channel	Size	Storage issues for nodes and networks requiring greater bandwidth

TABLE II. COMPARISON OF DIFFERENT CONSENSUS APPROACHES FOR SPECIFIC USE-CASES [11]

Management entity	None	**Single organisation**	**Multiple organisations**
Network type	Public	Private	Hybrid: public and private
Participants	Anonymous	Identified and trusted	
Consensus mechanism	Mining e.g. *proof of work*	Multi-party consensus algorithm	
Transaction approval time	Long, e.g. 10 minutes	Short, e.g. 100ms	
Use cases	1. Currency payments; 2. Certifying product authenticity; 3. Global identity management	1. Interbank settlement; 2. Supply chain traceability; 3. Medical and military records	
Examples	Bitcoin, Ethereum	Hyperledger Fabric	

III. PATIENT RIGHTS AND PRIVACY

In the EU, the sharing and access of health-data by data-controllers is subject to the General Data Protection Regulation (GDPR) which provides subject data rights to EU citizens [14]. Unlike the Health Insurance Portability and Accountability Act (HIPAA) [15], which sets the standards that regulate how patient medical records and related medical information is used within the US, GDPR is much broader in scope. GDPR covers all personally identifiable information (PII) used by third-party organisations rather than only protected *health* information (PHI) as is the case with HIPAA.

While regulatory agencies do not create technical standards, to have efficient blockchain integration within large scale healthcare applications, technical standards and regulatory policies must operate hand-in-hand; between interoperability standards such as openEHR, engineered blockchain infrastructures, and GDPR. For example, three GDPR articles seemingly conflict directly with blockchain implementations as, by definition, on-chain data is unalterable upon confirmation by the network:

- Right to rectification: data can easily be added to a blockchain but not altered
- Right to erasure: data cannot be removed once confirmed
- Right to restrict processing: there is little control over what nodes are processing the data

The customisability of blockchain designs allows for some possible solutions to these problems. One option is that a blockchain that contains health information must keep only encrypted rather than explicit PII, which individuals can subsequently unlock using a decryption key that only they own. However, this is not suitable as blockchains are notoriously ill-equipped to handle large volumes of data at scale [16]. Instead, a hybrid blockchain design storing only a hash of a link to the location of off-chain health information is a much more suitable and deliverable solution. A schematic illustration of this model is depicted in Fig. 1. As the on-chain hash is one-way, original information containing PII cannot be reconstructed from it alone, yet, the hash can still verify the off-chain information; providing rectification and erasure rights. Upon request, PII residing on central servers can be removed leaving the on-chain hashes indexing no information. By nature of participants being known and trusted, the restriction of data processing is also made possible.

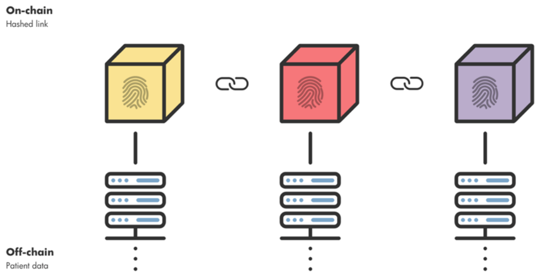

Figure 1. A hybrid blockchain design containing a hashed soft-link to off-chain patient information.

Under a hybrid on-chain gateway to off-chain PII model, a layer of functionality is made possible that is GDPR compliant and operates on top of existing health infrastructural blueprints. Beyond minimal compliance, this implementation may promote patient's GDPR rights:

- Right to be informed: individuals can see directly where their data is and how it is accessed
- Right to access: Beyond a subject access request, individuals are provided with an intrinsic gateway to their record. Patients have read-access and can give read-write permissions to clinicians
- Right to object: Transparency can be generated between health vendors and individuals
- Right to data portability: Data can be obtained through the gateway in a simple format

We now consider the extent to which distributed accessibility of health information may influence health data security.

IV. HEALTHCARE DATA SECURITY

With greater health-data accessibility and the increased ability to share healthcare data, data security requirements increase accordingly.

Between 2013 and 2017, hacking was responsible for nearly 85% of all affected patient records in the US. This is a major global issue [9]. In May 2017, the infamous WannaCry ransomware attack hit 35% of UK hospital trusts and 8% of general practices; affecting approximately 1% of all NHS care for a week - the largest recorded cyber-attack to ever affect the NHS [17]. The subsequent cost was £92m; £20m for 19,000 cancelled appointments and £72m in the subsequent clean-up and IT system upgrades. This highlights just how devastating a single cyber attack can be, both fiscally and to the potential risk of patients [18], as a simple result of outdated hospital IT systems. Some breech cost estimates have been reported in the literature as high as $355 per breached patient record [19]. Furthermore, these increasing trends in digital health information security risks are important when considering GDPR legislation, as, unlike HIPAA which allows organisations 60 days from the discovery a breach to notify affected parties, under GDPR organisations have only 72 hours. Growing numbers of complex breach attempts, the associated monetary penalty associated alongside pressure to act rapidly are all valid motivations for openness about novel security solutions in healthcare data.

As outlined previously, a key benefit of blockchain as opposed to traditional databases relates to its use of cryptographic algorithms intrinsic to its function to improve security and, in specific designs, privacy. For example, the cryptocurrency bitcoin blockchain utilises the 256-bit Secure Hash Algorithm (SHA-256), a cryptogenic hash function. This algorithm is also used in the generation of user addresses for privacy, as each user is represented by a hash value rather than their real identity [20].

Importantly, distributed methods for data integrity validation are not alone sufficient to solve all cybersecurity hazards. Cybersecurity requires a holistic approach, viewed beyond a technical challenge alone to also being a business risk with board-level involvement and expert involvement to address specific security challenges and many more precautions.

V. Conclusion and Future Work

The ultimate goal for blockchain utilised in the ways described in this paper, and beyond, is to improve healthcare processes and thus patient outcomes. Blockchain can help in multiple ways; lowering transaction costs by the use of smart contracts (embedded general-purpose protocols [21]) to automate processes, reduce administrative burden and remove intermediaries. Other blockchain endeavours seek to enable better health data collection, utilisation and sharing from patients, researchers and data sub-processors.

Looking forward, ongoing research leading to peer-reviewed publications and real-world examples may further delineate the use of blockchain within healthcare. We can be hopeful that patient centred blockchain designs empower patients to give explicit consent rights to read and share their healthcare data, whilst providing write access to healthcare professionals. Audit trails for when, whom-by and where health data has been accessed can be more seamlessly generated. Overall, this may make healthcare much more transparent than is currently the case.

Blockchain technology can surmount the stake-holder centric nature of healthcare data silos and enable anonymous verified health data exchange markets driven by patients themselves. This health data marketplace would consist of clinically verified and validated data, including treatments, diagnostics and genetic profiles. This may empower patients who are incentivised to contribute to their treatment, and further research - by giving portability to their patient records which can inform research, clinical trial matching, or access to experimental treatments.

Blockchain distributed ledger technology can advance healthcare in a number of currently unknown ways, and we expect many new applications to emerge in the coming years.

References

[1] Department of Health & Social Care, “The future of healthcare: our vision for digital, data and technology in health and care,” Oct-2018. [Online]. Available: https://www.gov.uk/government/publications/the-future-of-healthcare-our-vision-for-digital-data-and-technology-in-health-and-care/the-future-of-healthcare-our-vision-for-digital-data-and-technology-in-health-and-care. [Accessed: 05-Apr-2019].

[2] NHS, “Personalised Health and Care 2020 Using Data and Technology to Transform Outcomes for Patients and Citizens A Framework for Action,” 2014.

[3] I. McNicoll, A. Mehrkar, and T. Shannon, “FHIR ® and openEHR,” 2019.

[4] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System.”

[5] Medicalchain, “Medicalchain - Blockchain for electronic health records.” [Online]. Available: https://medicalchain.com/en/. [Accessed: 05-Apr-2019].

[6] Medibloc, “Medibloc.” [Online]. Available: https://medibloc.org/en/. [Accessed: 05-Apr-2019].

[7] e-Estonia, “e-Health Records — e-Estonia.” [Online]. Available: https://e-estonia.com/solutions/healthcare/e-health-record/. [Accessed: 05-Apr-2019].

[8] P. Densen, “Challenges and opportunities facing medical education.,” *Trans. Am. Clin. Climatol. Assoc.*, vol. 122, pp. 48–58, 2011.

[9] J. G. Ronquillo, J. Erik Winterholler, K. Cwikla, R. Szymanski, and C. Levy, “Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information,” *JAMIA Open*, vol. 1, no. 1, pp. 15–19, Jul. 2018.

[10] openEHR, “openEHR.org.” [Online]. Available: https://www.openehr.org/. [Accessed: 05-Apr-2019].

[11] FHIR, “FHIR v4.0.0.” [Online]. Available: https://www.hl7.org/fhir/. [Accessed: 05-Apr-2019].

[12] X. P. Akarca D, Saleh K, “Upgrading our digital health infrastructures with blockchain-based records,” *Cambridge Med. J.*, 2018.

[13] Vince Tabora, “Databases and Blockchains, The Difference Is In Their Purpose And Design.” [Online]. Available: https://hackernoon.com/databases-and-blockchains-the-difference-is-in-their-purpose-and-design-56ba6335778b. [Accessed: 05-Apr-2019].

[14] EUGDPR, “EUGDPR – Information Portal.” [Online]. Available: https://eugdpr.org/. [Accessed: 05-Apr-2019].

[15] HIPAA, “HIPAA Journal - News and articles about HIPAA.” [Online]. Available: https://www.hipaajournal.com/. [Accessed: 05-Apr-2019].

[16] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, “Where Is Current Research on Blockchain Technology?—A Systematic Review,” *PLoS One*, vol. 11, no. 10, p. e0163477, Oct. 2016.

[17] National Audit Office, “Investigation: WannaCry cyber attack and the NHS A picture of the National Audit Office logo.”

[18] R. Clarke and T. Youngstein, “Cyberattack on Britain’s National Health Service — A Wake-up Call for Modern Medicine,” *N. Engl. J. Med.*, vol. 377, no. 5, pp. 409–411, Aug. 2017.

[19] IBM, “Cost of a Data Breach Study - Global Overview,” 2018.

[20] Bitcoin Wiki, “SHA-256 - Bitcoin Wiki.” [Online]. Available: https://en.bitcoin.it/wiki/SHA-256. [Accessed: 05-Apr-2019].

[21] P. Cuccuru, “Beyond bitcoin: an early overview on smart contracts,” *Int. J. Law Inf. Technol.*, vol. 25, no. 3, pp. 179–195, 2017.