Towards a Blockchain-Based Healthcare Information System

Vojislav B. Mišić*, Jelena Mišić*, and Xiaolin Chang†
*Ryerson University, Toronto, ON, Canada
†Beijing Jiaotong University, Beijing, China

***Abstract*—Healthcare information systems are the next big application area for Blockchain technology. However, straightforward extensions of existing digital cryptocurrency systems such as Bitcoin and Ethereum results in systems that are unsuitable for the challenges posed by healthcare systems. In this paper, we propose an architecture for a blockchain-based healthcare information system in which block validation is performed through collective signatures initiated by a designated leader and executed by a pool of witnesses. Furthermore, we describe a smart-contract based approach that allows data owners to explicitly grant or revoke authorizations for other actors to access healthcare data. All accesses, successful or not, are recorded on the blockchain as separate transactions, thus ensuring transparency and privacy protection.**

I. Introduction

Blockchain has received much attention ever since the appearance of digital crypto-currency Bitcoin [1] but many other areas seem poised to profit from this technology, including health and medical information systems [2]. A number of recent papers have proposed blockchain-based healthcare systems and/or highlighted some of their pertinent properties [3], [4], [5], [6], [7]. A brief overview of some of these proposals (and some partially implemented systems) is given in [8].

However, most of these solutions are straightforward extensions of existing digital cryptocurrency systems such as Bitcoin [1] and Ethereum [9]. As such, they don't quite fit the requirements for healthcare data which are rather different from those for a digital cryptocurrency. Two of the areas in which such differences are rather striking are validation of blocks containing healthcare data and privacy protection of that data.

Cryptocurrencies perform validation by 'mining' transaction blocks, typically by using Proof-of-Work (PoW) principle [10]. For example, Bitcoin blocks are mined by solving a cryptographic puzzle, the difficulty of which is periodically adjusted to maintain a constant (and, perhaps, artificially low) average rate of block mining. This approach makes little sense if the blockchain is to contain healthcare data. First and foremost, validating a block of medical records necessitates expert medical knowledge, rather than simple arithmetic that suffices for a cryptocurrency. Second, limited block validation rate is unsuitable for healthcare data, as time is of the essence in many medical scenarios. Last but not least, computational and energy expenditure needed for PoW validation is excessive, esp. when considering that the Bitcoin blockchain can achieve only statistical consistency – i.e., it is never finalized.

As for privacy, cryptocurrencies typically protect the identity of transaction participants by public key cryptography but leave the content of monetary transactions in the clear. On the contrary, in a healthcare information system both the identity of participants, in particular that of the patient, and the actual content of a transaction – be it a physician's diagnosis, an examination report, or a prescription to be filled – should be protected from unauthorized access. Furthermore, a number of other constraints apply, as elaborated in Section II below.

In this paper, we propose efficient solutions for these problems. Transactions and blocks are validated by collective signatures [11] which is efficient in terms of computational and communication workload and allows for easy verification later on. Block validation is conducted by a dynamic group of witnesses with a rotating leader role, which ensures the participation of all users as well as sharing of the communication workload. Privacy is ensured by using an ElGamal encryption system with non-global escrow [12]. In this approach, each user has a public key with two corresponding private keys, one that can be used for both signing and encryption, and the other that can be used only for decryption. The latter key can be escrowed with a trusted third party and used to decrypt the data when needed. We outline the procedures to implement such a system and highlight its pros and cons in practice.

The rest of the paper is organized as follows. Section II outlines security and privacy requirements for health information. Section III gives a brief introduction to blockchain technology and argues that straightforward use of cryptocurrency techniques is unsuitable for a healthcare information system. The proposed system and its constituent parts, as well as its operation, are described in detail in Section IV. Finally, Section V concludes the paper and outlines the directions for further research.

II. Data privacy requirements for health information

The foremost principle regulating access to health information is that health records are considered to be the property of the patient, in accordance with the applicable laws such as the Personal Health Information Protection Act (PHIPA) in Ontario [13], and similar legislation enacted throughout Canada and elsewhere.

Consequently, the patient must have access to all of their records at any time, subject to certain legally defined exceptions [14]. Access to health records must be limited to

individuals and/or entities explicitly authorized by the patient. Right to access the data may be given for all health data or just to specific information such as diagnoses, prescriptions, or examination and test results. By extension, the patient should be able to modify or revoke any access rights they have previously granted. If the patient is temporarily or permanently incapacitated, the authority to grant or deny access should rest with the legal guardian or another person with the appropriate power of attorney. In case of an emergency, clinicians should be able to apply the so-called break-the-glass rule in order to access patient's records. In all cases, the patient must be notified of any access to their records.

Protection of patient data may be accomplished by encrypting the data with a key known only to the patient, and subsequent access to the data should be possible only 'by parties that have the patient's private key' [2]. However, when the patient authorizes an actor to access their records by passing on their private key, all of patient's data stored in the system becomes accessible to that actor. Furthermore, the actor would be able perform any action that the patient is capable of performing, including signing subsequent transactions, authorizing access, and the like. Obviously a way must be found to allow access to data without giving away other privileges that the patient normally enjoys.

Revocation of access privilege poses another challenge, namely, how can an actor 'forget' the private key previously given by the patient? The simplest solution is to issue a new private key to the patient, but the actor in question would still have access to all data protected by the old key, while all other actors that are to retain their authorization must be given the new private key.

Furthermore, the ability to control access implies cryptographic protection of all health data and restriction of access to explicitly authorized actors (e.g., physicians, nurses, lab technicians) only [15], [16]. But unlike other types of information, health records need to be kept and access-protected for a long time. Maintaining cryptographic protection, then, means that the system should maintain the ability to decrypt and access any record for years or even decades. This is a serious challenge that can be mitigated by escrowing the patient's private key at a trusted party.

We also note that the health information system should protect the integrity of the patient's medical record through the so-called confinement rule which states that 'information from one medical record may not be appended to another one' [17], even if all the actors authorized to access the latter are also authorized to access the former. This rule applies to the scenario in which the patient revokes some actor's access rights to one or the other of the original records at a later time, and the actor attempts to access the aggregated record; if the confinement rule is enforced, this should result in access rights violation.

III. Blockchain to the rescue . . . or not?

Blockchain is a data structure composed of blocks with arbitrary content, typically a set of 'transactions.' Each block is identified by its hash, which is also used for linking to the next block in the chain so that the blocks effectively form a backward linked list. The first (oldest) block is oftentimes referred to as 'genesis' block and it is typically created by the software package that manages the chain, as is the case with Bitcoin [1].

Resistance to tampering, often incorrectly referred to as 'immutability,' is provided through a data structure known as the Merkle or hash tree [18] to the block header. The Merkle tree is a binary tree in which leaves are actual transactions, and nodes higher up in the tree are formed by hashing together the hashes of the two nodes below. The header of each block in the chain includes the root of the Merkle tree computed from all transactions in the block. Any tampering with the contents of the block will render the Merkle tree root invalid, which can be easily checked by comparing the stored Merkle tree root with the one calculated from the actual block.

Replicating the blockchain ledgers on many nodes in a decentralized, peer-to-peer (P2P) network provides additional resistance to tampering. Subverting a single node in this setup would do little harm as all other replicas would still contain the correct data. An attacker would, thus, have to subvert a majority of the nodes in order to force a change in the ledger content. This is theoretically possible but rather hard to achieve in practice as different replicas are maintained by independent and, most likely, geographically scattered entities.

The properties described above make blockchain a promising choice for health record maintenance and sharing [2]. However, straightforward application of blockchain technology for crypto-currencies leads to a number of theoretical as well as practical shortcomings that are not adequately addressed.

A typical architecture for a blockchain-based health record system is based on a single public blockchain ledger replicated across all nodes. Unlike Bitcoin and other crypto-currencies, nodes must be authorized to access the ledger, which means that a permissioned approach is used.

Transactions are created and broadcast to other nodes in the network by the electronic health record (EHR) system operated by a healthcare provider such as a physician, nurse, pharmacist, or some other actor in the healthcare system. Patients access the data through similar, possibly less computationally capable systems, oftentimes referred to as personal health record (PHR) clients. Transactions are stored using a suitable format which may be machine-readable, human-readable, or both; in the last case, the HL7-proposed Consolidated Clinical Document Architecture (C-CDA) which is an XML-compliant document structure standard seems like a viable choice [19]. Unlike Bitcoin and other crypto-currencies, the actual content of each transaction must be protected against unauthorized access through encryption.

Transactions are subsequently packaged into blocks which are 'mined' and validated according to the rules of the blockchain system used. Once a sufficient number of nodes validates the block containing the transaction, it is permanently committed and becomes a part of patient's health record.

Validating or committing a block of transactions to the blockchain is not well defined in most proposals; a typical solution is to use a consensus-based protocol similar to the

Proof-of-Work approach in Bitcoin. However, it is unclear how many nodes need to validate the block for it to become valid. It is certainly infeasible to require that all nodes take part in validating a block, but the number of validating nodes should not be too small either. And if Proof-of-Work or similar approach to consensus is used, who will provide the computing power necessary for validation?

The vague definition of majority also means it is unclear how much time it will take for a transaction to become publicly validated as part of the 'official' chain. Would the transaction be available to actors other than those involved in creating it during that process, or not? Note that time may be of essence in certain medical scenarios, and making the data unavailable for even a short period of time may endanger the patient's health or even lead to life-threatening delays in providing the necessary medical care.

In fact, it is questionable whether the mechanism for block validation for a crypto-currency should be applied to a blockchain containing medical records. Namely, validation in applications such as Bitcoin or Ethereum includes checking the amounts (i.e., unspent transaction outputs, or UTXOs) or account balances. However, health data does not include any currency amounts; instead, it is comprised of examination results, laboratory tests, or diagnostic information. This data could be validated by another physician or laboratory, but not without another examination or laboratory test.

In view of the issues listed above, it is certain that a different solution is needed – one that will take into account the specific requirements of healthcare systems. We will now describe such a solution.

IV. The proposed system

A. Architecture

The proposed architecture consists of different actors operating their own EHR/PHR applications on different hardware systems, as shown in Fig. 1. These systems are interconnected through the Internet, possibly with the use of a Virtual Private Network (VPN) that provides the first line of defense against unauthorized access. Individual users must log in to their respective EHR/PHR systems in order to create and record health information during appropriate interaction with other actor or actors.

Unlike most digital crypto-currencies, all actors – be they healthcare providers, practitioners, pharmacists, insurance providers, or patients – must be explicitly authorized to access and use the system. Authorization may be provided by a central authority such as a government agency which certifies healthcare practitioners (physicians, nurses, ...) anyway. Note that in some jurisdictions there may be several such agencies, in which case the use of a replicated, tamper-proof, yet easy to access ledger storing all the authorizations (and, possibly, subsequent revocations of some of them) would be most welcome [20]. Such an authority could also provide authorization for the patients when they register to use the blockchain-based system. For example, all residents in Ontario are entitled to Ontario Health Insurance Plan [21] which covers basic health services; additional services may be covered by employment-based or individual insurance contracts.

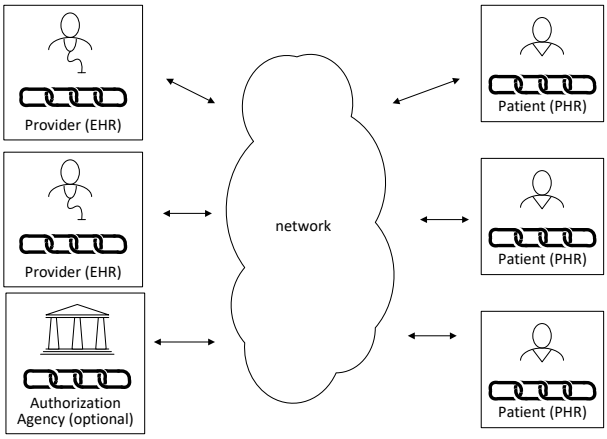


Fig. 1. System architecture (after [2]).

It may be tempting to require that each patient maintains their own private blockchain on a private smart device, but this solution may not be affordable or, indeed, feasible, as storage space of current smart devices would not be able to store the entire ledger. Instead, patients' blockchains may be operated and maintained by a third party; individual patients could use a device such as a smartcard or a bracelet to identify themselves when they need to interact with the system [22]. In jurisdictions where the government-sponsored universal healthcare is available, such a software system could be operated by the appropriate government agency. In present systems of this kind, those government agencies already store a large portion of health data, and patients already have identification cards or similar devices. The crucial difference is that the new system must include mechanisms to allow patient to access their own data and control access to it by other actors in the system.

Alternatively, individual parties' blockchains could be managed by an intermediary, most likely a for-profit organization acting as a 'health data provider.' Given that many current organizations already provide substantial cloud-based storage and computational resources, together with a suite of related applications, this solution seems quite feasible. The government agencies would still play an important role in certifying health care providers and making sure that their software tools manipulate and store health data records in accordance with the relevant regulations.

B. Transactions

Each transaction has one or more participating users: for example, a visit transaction involves a patient, a physician or perhaps more of them, and a nurse or several nurses; a prescription transaction involves a patient, the prescribing physician, and eventually the pharmacist providing the prescription medication; and a laboratory examination transaction involves a patient, the referring physician, the laboratory physician (or physicians), nurse or nurses, and/or laboratory technician(s). Authorization transactions will be created by the patient or their legal representative.

Each transaction must be signed by all participants, using a suitable collective signature protocol such as the one described

in [11] which uses Schnorr multisignature [23], or the recently proposed compact multisignature described in [24]. In most cases the number of signing parties will be low and the signing process can be performed quickly.

We note that an interaction between a patient and a healthcare provider may result in a chain of subsequent events. For example, a visit to the doctor may lead to a prescription which is then fulfilled, or a referral to another physician which then results in another visit. It may be tempting to try to store the information about all related events in a single transaction. As these events occur at different times, it would be counterproductive to keep a transaction 'open' for a long time before it is checked and broadcast to the network. Instead, each interaction or event should be recorded in a separate transaction. Links to earlier transactions, if needed, are implemented as references within the transaction itself. In line with the blockchain philosophy, all references to objects are, in fact, hashes of their respective contents.

Some transactions contain forward references such as a referral for a laboratory test or a specialist examination. This should be recorded as a note in the transaction content, rather than through an actual reference to the provider. The rationale behind this is as follows. In some cases, the exact identity or location of that provider may not be known at the time the transaction is recorded: e.g., a prescription for a medication may be fulfilled at any pharmacy. In other cases, the provider identity is known but that of the actual practitioner is not: e.g., a patient may be referred to a clinic but it is not known who will perform the examination. Finally, sometimes the referral is addressed to a practitioner that is not available when the patient shows up, in which case another practitioner with equivalent credentials will undertake the necessary actions. Either way, the inclusion of a specific identifier of the provider would be rendered invalid.

The structure of a transaction is schematically shown in Fig. 2(a).

C. Transaction types

In the proposed system, we can identify a number of transaction types, as follows.

An *association* transaction, somewhat similar to a genesis block in Bitcoin, records the first appearance of an actor in the system, be it a patient or a clinician, or a healthcare provider. It thus involves that actor and the authorization agency.

An *authorization* transaction is entered by the patient when she or he desires to enter into a relationship with a healthcare provider. It may authorize one or more specific healthcare providers to access some or all of patient's health records. In the former case, the authorization may refer to a specific transaction or a set of transactions, perhaps within an explicitly specified range of dates or chosen according to some other criteria. An authorization transaction may also revoke an existing authorization.

Authorization transactions may actually refer to a healthcare provider organization rather than a specific individual. In that case, the authorization should be inheritable by individuals working in appropriate capacity. For example, a referral for a laboratory exam will often refer to a laboratory rather than a specific laboratory technician, and sometimes just to a type of test.

A *delegation* transaction is similar to the authorization transaction but it applies to the implementation domain. In this case, the patient may authorize (or de-authorize) their health data provider to operate the blockchain-based health record system on patient's behalf. The allowed operations include signing of transactions, initiating transactions, and validation of blocks of transactions. This type of transaction is particularly interesting in case a patient doesn't own or doesn't want to use a smart device with the appropriate PHR client application. Ideally, a valid delegation transaction does not preclude direct patient access and management of health information, and patients can enjoy the full functionality of the system, except that their requests may have to be fulfilled by the personnel of their health data provider.

An *access* transaction is a record of an actor attempting access to a specific data item related to another actor, similar to the approach proposed in [25]. In most cases, this would involve a physical or a nurse accessing patient's data, but other cases are also possible. For example, a patient may want to check the proposed another actor's authorization in the particular organization. Either way, the access transaction should also record whether the request has been granted or denied, and if so, on what grounds.

Other, more specific types of transactions may be defined as appropriate.

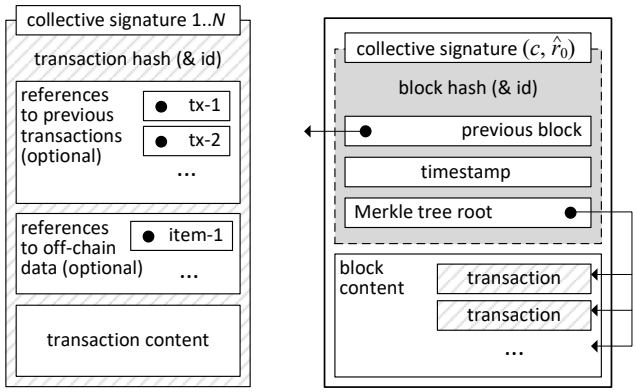
D. Transaction protection

The actual content of the transaction should be encrypted to protect the privacy of patient's data. To this end, we could use the patient's private key but this may be too restrictive, as the practitioners that have created the data in the first place would still obtain permission to access it, which makes little sense.

To mitigate possible loss of this key and to facilitate access, the patient may entrust their private key to a third party such as the authorization agency. This would turn the authorization agency into a key escrow which is a single point of failure and a target for attacks [26]. As the proposed blockchain system is permissioned, an attacker would need to gain access to the authorization agency prior to launching any attacks, but this is not an insurmountable obstacle.

A variation of this approach would use an encryption system such as XTR in which each user has a public key with two corresponding private keys [12]. In this scheme, the user uses their private key to both encrypt the data and sign it, while the other private key can only be used to decrypt the data but not sign it, and hence it can be given to an escrow. In this scheme, losing either of the private keys means that a new set of public/private keys must be generated but the data would still remain accessible through the other private key. Of course, generation/issuing of a new set of keys may require physical interaction of the individual (or their representative) with the authorization agency.

Alternatively, the participants in the transaction could agree on a shared key for the transaction in question. Again, this



(a) Structure of a transaction. (b) Structure of a block.

Fig. 2. Transaction and block structure.

necessitates that some entity acts as a key escrow, since the actual transaction content needs to be accessible at a later time and, possibly, to a third party which was not privy to the original transaction, upon a properly authorized request.

Finally, it is also possible to leave the transaction content in plaintext, as is the case with Bitcoin. As the participants are known only through their public keys, this solution is not so insecure as it seems, the more so since we are dealing with a permissioned system.

As noted above, large items such as ultrasound or X-ray imagery should be stored by the healthcare provider that has created the items in the first place. As such provider must have had access to the item in the process of creating it, there is no violation of patient's data privacy. However, the data must remain accessible only upon an authorized request.

E. Blocks and block validation

When a transaction is created and signed, it is broadcast to the network so that any of the actors in the system can validate it. As explained above, the contents of a healthcare transaction does not need validation, even if it were not encrypted; instead, validation involves checking the validity of participants' signatures and the resulting hash value.

A number of transactions is put together in a block and validated. Unlike the Proof-of-Work-based blockchain systems, computationally intensive and competitive block mining by just about any actor is not an option. Instead, we could use the collective signing protocol proposed by [11], [27] which is initiated by a designated 'leader' and supported by a set of 'witnesses.'

The number of witnesses should be chosen to reduce the likelihood of collusion among actors and/or of externally launched subversion attacks whilst at the same time keeping the latency of the signing process within reasonable limits. Since the number of actors is large, the solution in which all actors act as witnesses for each newly proposed block, as in the well known solutions [28], [29] to the Byzantine Agreement Problem [30], is not feasible.

Two problems that need to be solved are the selection of the leader and the witness pool for block validation. We propose a solution that aligns with the Proof-of-Stake principle [31]: namely, both the leader and the witnesses should be selected from the set of actors with the highest stake – in other words, from the set of actors that have participated in the largest number of transactions awaiting blocking and validation. Such data is readily available since all transactions are broadcast to the network as soon as they are signed.

The new leader and the new witness pool may be appointed by the current leader after each successfully validated block, as in Bitcoin, or after a number of blocks have been validated, as in Bitcoin-NG [32]. The latter option has the advantage of spreading the overhead of leader and witness pool selection over a number of blocks. It is worth noting that, thanks to the use of collective signature protocol, the leader workload is not high – most of it is communication, rather than computation. Furthermore, the collective signature protocol is able to produce a valid signature even in case of absence of some of the witnesses [11].

Block validation and leader selection described above are summarized in Algorithm 1.

Algorithm 1: Block validation and leader selection.

Data: $mempool$ of unconfirmed transactions, $blockCounter$
Result: updated blockchain, $mempool$, $Leader$

if $mempool.size() > mempoolThreshold$ **then**
  assemble new $Block$;
  extract $Actors$ from transactions in the $Block$;
  select $Witnesses$ among $Actors$ with highest stake;
  get $Witnesses$ to collectively sign $Block$;
  broadcast $Block$ to all actors;
  $blockCounter++$;
  if $blockCounter > roundThreshold$ **then**
    select next $Leader$ among $Witnesses$;
    inform $Leader$;
  end
end

F. Accessing the data

Let us consider the case when an actor U want to access item x which is owned by another actor A. As mentioned above, any access to an item owned by A (typically, a patient) needs to be authorized by A and recorded in an access transaction stored in the blockchain.

To this end, U searches the blockchain looking for an authorization transaction $Au(U, A.x)$ authorizing U to access item $A.x$. The authorization may be explicit or implicit, by virtue of U's role or organization. The search proceeds from the most recent block backwards, as is 'natural' in a blockchain, and looks for the first applicable authorization transaction. Note that such a transaction may refer to several health data records, or even all of them, and it may also revoke an authorization that was previously granted. Either way, the first relevant authorization encountered in this search will be the most recent and, consequently, the currently valid one.

If the authorization is positive, i.e., if it grants U the right to access item $A.x$, U will then conduct another search of its blockchain, again beginning from the most recent block, to find the transaction containing the requested item x. This

procedure may be effectively executed using a smart contract [9] that will perform the search. If the item is found, it is decrypted and returned to the user; if not, a message 'item not found' is sent.

If an appropriate authorization is not found or if U is explicitly prohibited from accessing the item $A.x$, a message 'access not permitted' is sent back.

Either way, the smart contract will record the request for a data item and its outcome, and package it in a data access transaction which is then broadcast to all users, thus creating an audit trail of all access requests. In this manner, data owners and/or authorization agencies can effectively track all accesses to data.

We note that revocation of an authorization does not seem to be a very common option. Moreover, the fact that all accesses are recorded seems to be a serviceable deterrent against unauthorized access, although its effectiveness probably deserves more investigation.

V. Conclusion

Blockchain technology offers an attractive solution for the design of next-generation healthcare information systems. However, such systems pose a number of challenges that cannot be solved by simply applying the solutions that were developed for crypto-currency applications. Instead, the specific requirements of healthcare systems need to be considered in the development of blockchain-based systems from the ground up. In particular, healthcare data which is the property of individual patients should remain accessible to them at all times, and all accesses to it must be governed by explicit authorization by the individual who owns it. In this paper we have described the basic tenets of such a system which addresses those requirements whilst ensuring that the benefits of using the blockchain – most notably, resistance to tampering, fast processing, and authorized (and recorded) access, remain available at all times.

References

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.

[2] Drew Ivan. Moving toward a blockchain-based method for the secure storage of patient records. In *ONC/NIST Use of Blockchain for Healthcare and Research Workshop. Gaithersburg, Maryland, United States: ONC/NIST*, 2016.

[3] Suveen Angraal, Harlan M. Krumholz, and Wade L. Schulz. Blockchain technology: applications in health care. *Circulation: Cardiovascular Quality and Outcomes*, 10(9):e003800, 2017.

[4] James Brogan, Immanuel Baskaran, and Navin Ramachandran. Authenticating health activity data using distributed ledger technologies. *Computational and Structural Biotechnology Journal*, 16:257–266, 2018.

[5] Ariel Ekblaw, Asaph Azaria, John D Halamka, and Andrew Lippman. A case study for blockchain in healthcare: "MedRec" prototype for electronic health records and medical research data. In *Proceedings of IEEE open & big data conference*, volume 13, page 13, 2016.

[6] Joshua C. Mandel, David A. Kreda, Kenneth D. Mandl, Isaac S. Kohane, and Rachel B. Ramoni. SMART on FHIR: a standards-based, interoperable apps platform for electronic health records. *Journal of the American Medical Informatics Association*, 23(5):899–908, 2016.

[7] Aiqing Zhang and Xiaodong Lin. Towards secure and privacy-preserving data sharing in e-Health systems via consortium blockchain. *Journal of medical systems*, 42(8):140, 2018.

[8] Matthias Mettler. Blockchain technology in healthcare: The revolution starts here. In *e-Health Networking, Applications and Services (Healthcom), 2016 IEEE 18th Int. Conf.*, pages 1–3. IEEE, 2016.

[9] Vitalik Buterin. Ethereum: A next-generation smart contract and decentralized application platform, 2017. http://ethereum.org/ethereum.html.

[10] Marko Vukolić. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. In *International Workshop on Open Problems in Network Security*, pages 112–125. Springer, 2015.

[11] Ewa Syta, Iulia Tamas, Dylan Visher, David Isaac Wolinsky, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, Ismail Khoffi, and Bryan Ford. Keeping authorities "honest or bust" with decentralized witness cosigning. In *Security and Privacy (SP), 2016 IEEE Symposium on*, pages 526–545, 2016.

[12] Eric R. Verheul. Evidence that XTR is more secure than supersingular elliptic curve cryptosystems. *Journal of Cryptology*, 17(4):277–296, 2004.

[13] Ontario. The Personal Health Information Protection Act (PHIPA), May 7, 2018. http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm.

[14] B. Dickens. Medical Records-Patient's Right to Receive Copies–Physician's Fiduciary Duty of Disclosure: McInerney v. MacDonald. *Canadian Bar Review*, 73:234, 1994.

[15] Ross J. Anderson. A security policy model for clinical information systems. In *Int. Symposium on Security and Privacy*. IEEE, 1996.

[16] Matt Bishop. *Computer Security – Art and Science*. Pearson Education, Inc., Boston, MA, 1st edition, 2003.

[17] Jelena Mišić and Vojislav B Mišić. Implementation of security policy for clinical information systems over wireless sensor networks. *Ad Hoc Networks*, 5(1):134–144, 2007.

[18] Ralph C. Merkle. Protocols for public key cryptosystems. In *Security and Privacy, 1980 IEEE Symposium on*, pages 122–122. IEEE, 1980.

[19] Robert H. Dolin, B. Rogers, and Charles Jaffe. Health level seven interoperability strategy: big data, incrementally structured. *Methods of information in medicine*, 54 1:75–82, 2015.

[20] Mark Hagland. In Nashville, a candid discussion of the potential for blockchain in healthcare, July 2018. https://www.healthcare-informatics.com/article/cybersecurity/nashville-candid-discussion-potential-blockchain-healthcare.

[21] Apply for OHIP and get a health card, 2018. https://www.ontario.ca/page/apply-ohip-and-get-health-card.

[22] Medicalchain SA. Medicalchain whitepaper 2.1, 2018. https://medicalchain.com/Medicalchain-Whitepaper-EN.pdf.

[23] Claus-Peter Schnorr. Efficient signature generation by smart cards. *Journal of cryptology*, 4(3):161–174, 1991.

[24] Dan Boneh, Manu Drijvers, and Gregory Neven. Compact multi-signatures for smaller blockchains. Cryptology ePrint Archive, Report 2018/483, 2018. https://eprint.iacr.org/2018/483.

[25] Guy Zyskind, Oz Nathan, and Alex Pentland. Decentralizing privacy: Using blockchain to protect personal data. In *Security and Privacy Workshops (SPW)*, pages 180–184, 2015.

[26] Bruce Schneier. *Applied Cryptography*. John Wiley & Sons, Inc., New York, N.Y., 2nd edition, 1996.

[27] Manu Drijvers, Kasra Edalatnejad, Bryan Ford, and Gregory Neven. Okamoto beats Schnorr: On the provable security of multi-signatures. Report 2018/417, IACR Cryptology ePrint Archive, 2018. http://eprint.iacr.org/2018/417.

[28] Miguel Castro and Barbara Liskov. Practical Byzantine fault tolerance. In *OSDI: Symposium on Operating Systems Design and Implementation*, 1999.

[29] Leslie Lamport. The part-time parliament. *ACM Transactions on Computer Systems (TOCS)*, 16(2):133–169, 1998.

[30] Leslie Lamport, Robert Shostak, and Marshall Pease. The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3):382–401, 1982.

[31] Shehar Bano, Alberto Sonnino, Mustafa Al-Bassam, Sarah Azouvi, Patrick McCorry, Sarah Meiklejohn, and George Danezis. SoK: Consensus in the age of blockchains. *arXiv preprint arXiv:1711.03936*, 2017.

[32] Ittay Eyal, Adem Efe Gencer, Emin Gün Sirer, and Robbert Van Renesse. Bitcoin-NG: A scalable blockchain protocol. In *NSDI*, pages 45–59, 2016.