# Blockchain for E-Health-Care Systems: Easier Said Than Done

**Article** *in* Computer · July 2020

DOI: 10.1109/MC.2020.2989781



**4 authors:**

Sujit Biswas
Faridpur Engineering College ( University of Dhaka)
**18** PUBLICATIONS **197** CITATIONS
SEE PROFILE

Kashif Sharif
Beijing Institute of Technology
**71** PUBLICATIONS **758** CITATIONS
SEE PROFILE

Fan Li
Durham University
**62** PUBLICATIONS **1,927** CITATIONS
SEE PROFILE

Saraju P. Mohanty
University of North Texas
**462** PUBLICATIONS **5,457** CITATIONS
SEE PROFILE

# Blockchain for E-Healthcare Systems: Easier Said Than Done

Sujit Biswas, Kashif Sharif, Fan Li, Saraju P. Mohanty

**Abstract**—Blockchain (BC) as a Distributed Ledger Technology (DLT) can be very effective in providing access control and big data management in Healthcare systems. However, implementing a pure blockchain solution or migrating to one is an extremely challenging task. Several design and implementation dynamics should be considered before an efficient solution can be built.

**Index Terms**—Blockchain, Healthcare, Electronic Medical Records (EMR), Interoperability, Migration, Security, Privacy

BLOCKCHAIN has become a popular buzz word in recent years, giving the impression that it is a silver bullet to several (if not all) security problems. There is no denying that it does make systems more transparent, traceable, and secure, however, it is in no way a one-solution-fits-all technology. One can easily find several research works focused on using blockchain in different applications, ranging from industrial automation to vehicular networks, and from the Internet of Things to financial markets. From a practical perspective, these are easier said than done. In this work, we focus on the healthcare industry and explore how it can benefit from DLT in general and BC in specific for process automation, digital/electronic medical record management (including big data), access control, and smart contracts. Several works in literature have focused on these topics [1], [2], however, most of them solve very specific challenges while ignoring the related bigger picture. In this article, we first analyze and explain how business blockchain can be effectively used in healthcare, followed by the unique requirements of a healthcare system. In the latter parts of this article, we discuss the migration challenges and possible solution, the trade-off between unified and multi-chain environments, consensus algorithms for healthcare, users & access privileges, smart contracts, and e-healthcare specific industry regulations.

## DON'T THINK CRYPTO-CURRENCY

Blockchain has gained significant attention in the past few years, mainly due to sky-rocketing prices of Bitcoin. Since then, dozens of crypto-currencies have sprung-up around the globe. Perhaps the biggest misconception about blockchain is that it is for crypto-currencies only. Blockchain is primarily a Distributed Ledger Technology but has mostly been specialized for financial transactions. However, the generic DLT mainly focuses on providing a set of protocols and processes for the distribution of records among multiple nodes in a collaborating system [3]. The system may belong to a single enterprise, or multiple enterprises may connect to a single yet shared and distributed Ledger. Thus, blockchain inherits the benefits of DLTs and then adds a few more to the list, such as: Security through Smart Contracts which are predefined agreements between parties to conduct business, Transparency & Accountability through Immutable records stored at distributed locations, and Efficiency & Cost reduction due to automation of processes.

Blockchains for crypto-currencies revolve around the concept of tokens, which are exchanged among participating users. However, the benefits offered are not limited to tokens alone. Consider the token as a data element which is generated and traded while leaving an audit trail behind, then any digital asset (or piece of information) that is transferred among participants while requiring an audit trail, can potentially benefit from blockchain. Besides Access Control for such digital assets can be efficiently implemented through smart contracts while the data itself can be stored in the distributed ledger system increasing its reliability and authenticity. Based on these arguments, the use of blockchain beyond crypto-currencies is not only feasible but rather very practical. Business Blockchain (BBC) is a variant of traditional blockchain which aims at using the protocols of BC within a business process, such as collection of authenticated and verified data from assembly line sensors, casting and auditing of votes in an e-government solution, or asset tracking [4], [5]. Another method for classification of blockchain is based on the openness of the system; i.e. public, consortium/federated, or private blockchains. Public blockchains are open to all, while consortium is limited to a group of organizations and private to a specific organization. Public blockchains have publicly open access, and anyone can become a miner, peer, or trader. Contrarily, consortium/private usually have permissioned access, where users are first registered and authenticated. Business BC is usually consortium/private with permissioned access, where a peer is responsible for verification consensus formation [6].

Hyperledger [7] is a Linux foundation solution that can be used as a base platform for implementing business blockchains, hence most of the debate in this article involves its use and the flexibility it offers. It implements five frameworks intended for different types of environments and consensus mechanisms. Hyperledger Fabric is a major implementation that enables flexible consensus algorithm implementation, smart contract integration, and Internet of

*S. Biswas, K. Sharif, & F. Li are with Beijing Institute of Technology, China. S. P. Mohanty is with University of North Texas, USA.*

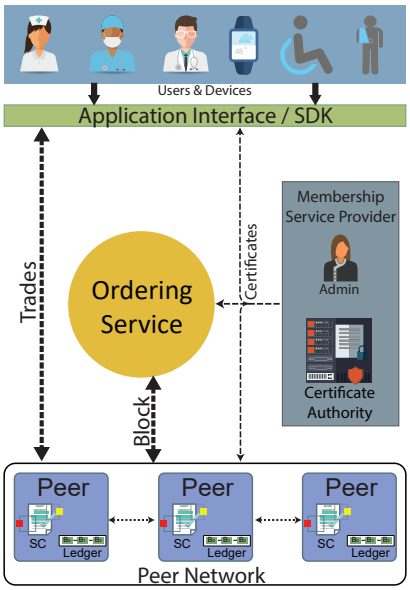


Fig. 1: The Business Blockchain Operational Framework.

Things (IoT) support. It is important to note, that it is only a platform, and does not provide a complete business solution for blockchain in any specific scenario.

## Healthcare Blockchains

Digitization and integration of the Internet of Things (IoT) in E-Healthcare Systems (eHS) have made it one of the fastest-growing domains, thus evolving to smart healthcare [8]. Statistics show that global healthcare spending will continue to increase in 2020 and beyond, with significant emphasis on digital transformation [9], [10]. The medical service providers will increase the use of innovative solutions, such as cloud computing, 5G, big data analytics, blockchain, artificial intelligence, etc. to reduce costs and improve the quality of care.

Integrating the blockchain with eHS can have several benefits, including but not limited to the security of electronic medical records (EMR), access control for different types of users, automated execution of services, remote data collection and logging, the unification or standardization of information, redundancy and fault tolerance, enforcement of healthcare regulations, logistics, etc. [11]–[13]. However, realizing such blockchain is extremely challenging. To begin with, a modern eHS is a combination of many different technologies at the device level as well as at the operational and management system level. Hence the blockchain solution should not only cater to the needs of small scale sensor device but should also accommodate devices which generate heavy images (CT scans). At the same time, this data has to be shared across departments, and with third-party service providers, such as insurance companies. To further complicate things, interoperability among different service providers may not be possible at all, due to completely different automation solutions.

To be more specific, some of the major challenges can be listed as: i) Existing centralized eHS store data in relational databases, whereas blockchain uses a file database and DB schema may not have a one-to-one mapping, ii) Due to restriction on transaction size in a block, it is impossible to store complete medical imagery as part of the chain, iii) Due to real-time transactions at a mass scale, it is challenging to migrate all medical history of patients to blockchain ledger, iv) In an eHS, it possible that some medical documents are paper-based. Hence the only way to digitize them is to store as images, which is a non-real time process, v) Access to patient data has to be tightly regulated for different types of internal and external users [14], vi) An eHS may allow integration of third-party IoT devices (smartwatch, health sensors) to be part of system, which makes verification and validation difficult, vii) Interaction with other non-BC subsystems of the e-healthcare ecosystem including regulatory bodies.

This is a non-exhaustive list of major challenges that arise when designing a complex blockchain solution for e-healthcare systems. In the following sections, we elaborate each and every aspect of designing such a system, and debate on the technical aspects of different solutions. It is important to note that the objective of this work is not to propose a complete solution, but to enable the audience in understanding what the challenges are, and what are the benefits of different possible solutions can be, although authors have inclination towards specific design choices.

Before proceeding, a generic business blockchain process is depicted in Figure 1. Users generate trades (transactions) containing digital assets that need to be shared with other users or devices. Membership Service Provider (MSP), comprises of an administrator and Certificate Authority (CA) responsible for providing keys, signatures, certificates, & configuration information. Peers are specialized nodes, with resources to execute consensus algorithms and maintain the distributed ledger. Ordering Service is responsible for grouping all endorsed/approved trades into a newly generated block. Smart contract or chaincode is deployed on the peer nodes for verification of transaction agreements between different users.

## EHR Privacy & Regulations

The primary reason to integrate blockchain into any system is the enhancement of security. It is important to understand that, BC only adds *validation* and *immutability*, to the asset *exchange process* and *stored data*, respectively. However, these additions have a significant and profound impact on the overall security architecture. The validation is done through smart contracts and consensus protocol that ensures that no illegal exchange happens, while immutability is achieved by hash connectivity in the chain ensures nothing is changed afterward. BC does not introduce any new encryption algorithm, signature mechanism, hash function, etc., hence, efficient use of existing or development of new algorithms in this regard is extremely important [15]. In an e-healthcare use case, several security & privacy primitives need to be reconsidered. For example, some BC systems (with public miners), allow the miners to read transaction payload, for validation and smart contract execution. In e-healthcare, this payload can be an EHR, which must not be shared (even in encrypted format). In a private blockchain, the compromised (or colluding) miner/peer cannot be ruled out.

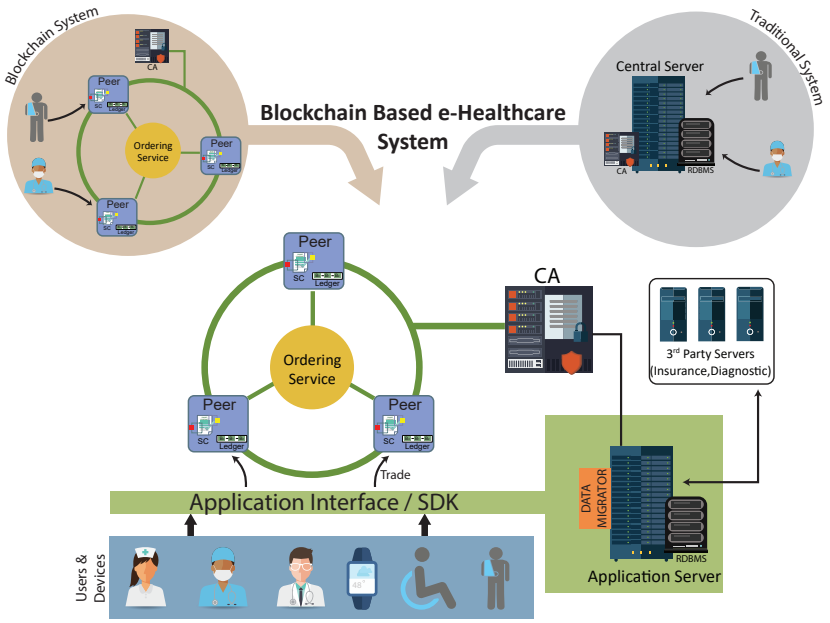


Fig. 2: A Blockchain-based Integration Framework.

Hence, the privacy of EHR may be compromised. Similarly, if the digital signatures used for validation can be linked to patients or their physicians, this may also contribute to a breach of privacy and healthcare regulations.

Based on this, two things must be considered before designing a BC-based e-healthcare system.

*i) Understanding of Regulations:* HIPAA [16] and GDPR [17] must be followed and misconceptions about both must be removed. For example, many researchers attribute GDPR with the *right to forget*, however, the regulation clearly states that for medical practitioners this is not an absolute right. Hence, data privacy as specified by HIPAA/GDPR must be enshrined in the system, for both internal and external elements.

*ii) Identification of Blockchain Use Case:* In light of privacy and regulations, it is imperative that the use of BC within the healthcare system must be identified. For example, consent management is a cornerstone of healthcare regulations. BC can be efficiently used for it. Similarly, access control to EHR, drug control, prescription administration, patient monitoring, insurance, and accounting, etc. where immutability and accountability are necessary, can significantly benefit from the blockchain.

Blockchain cannot be considered a blanket-solution for all healthcare sub-systems. The enforcement of regulations such as GDPR and HIPAA will be best done through smart contracts. Hence, mechanisms are needed that can guarantee that smart contracts are written in such a way to ensure the privacy regulations are met related to healthcare.

## Migration Issues

Designing and implementing any new system for a large or medium scale organization always requires crossover time with the old system. Slowly the old system is phased out while data and operations are migrated to the new. Most of the research in blockchain focuses on algorithmic technicalities and disregards the fact that the initialization time for a blockchain system especially for healthcare organizations may render the new solution infeasible. We approach this challenge from the following two aspects.

### Infrastructure and Architecture Changes

Traditional eHS systems are usually centralized as shown in Figure 2. The central application, its associated database, and perhaps the certificate authority all are hosted on a single server. The server may be in the cloud, but from the implementation perspective, it is still a centralized system. It is also possible that a large scale eHS provider has diversified locations, and thus has many centralized systems which collaborate at different levels. This creates an entirely different architecture, as the databases may be distributed while the web-based application may be centralized.

Compared to this, the blockchain system is entirely decentralized. Furthermore, this decentralization is not similar to decentralized database systems or distributed systems. As shown in Figure 2, the collection of peer nodes form a special peer network which performs consensus formation. While a specialized ordering service (a collection of orderer nodes) is responsible for block formation and its dissemination back to the peer network. Shifting from a centralized to a distributed blockchain requires significant changes in the infrastructure. This challenge has to be taken into account while designing the solutions. It is important to note, that the users or devices cannot initiate trades without an application interface. Many systems employ thin-clients on the user side, which means that there has to be an application server as part of the blockchain network. The majority of the research works trivialize this aspect, and users are assumed to be sending the trades directly to the peer. However, in reality, it may be the application server that does it. For thick-clients, this assumption may be completely safe, but the user devices would still interact with a system entity that manages access control. Figure 2 shows what a combined system would look like. It can be

intuitively observed that the application server can create a single point of failure, hence, it is important to remember that, just the use of blockchain does not make a system temper proof. This leads to several new challenges for securing and interfacing of blockchain with other systems, where secure & standardized APIs for system interaction should be developed.

### Data Synchronization and Migration

One of the least researched areas of blockchain implementation is the migration of existing records and databases to the new system. Perhaps the simplest reason is that the migration of records in their current form is not possible. First, the ledger is unable to accept the previous record with old timestamps. Every new transaction must have a current timestamp. Secondly, blockchain ledger is immutable, which means that any timestamp change after block creation is impossible. Hence any adjustment or updating has to be done before the migration starts. This is a non-trivial task and may change from one eHS to the other. Third, the traditional centralized system may have thousands of records for hundreds of patients. To bootstrap the blockchain system with all that data at initialization time can be a very long process. All the while the same system might be in use and creating (or possibly changing) the existing data. This creates a circular migration issue, which must be addressed at design time. Moreover, efficient migration algorithms and synchronization techniques are needed for this purpose.

One such possible solution is not to migrate the data at the initialization phase, but to migrate it only on need basis. As shown in Figure 2, a Data Migrator module can be used for formatting the relational database records into Ledger acceptable trades, only when needed. For example, a patient who has been visiting the eHS, has multiple records in the traditional system. After the blockchain migration, when the same patient visits the facility, only then the necessary records are synchronized. All new records are made in the blockchain system, while the relational database is only used as an old repository. This will ensure that the circular record updating is avoided, and initial bootstrap time is negligible. Efficient designs for such data migration interfaces and algorithms will be the key to successful migration.

## Unified or Multiple Blockchains

Blockchain solutions must be application-specific. In an e-healthcare scenario, there can be multiple service providers with their independent systems. Cooperation among these systems can be enabled if there is an operational level agreement. However, transferring EMR of a single patient to one another, or unifying them in a single database is often challenging. In a blockchain-based solution, this challenge is increased multi-fold.

First of all, if one service provider migrates to blockchain solution, then its operational cooperation with a traditional centralized service provider will immediately stop, as there is no default interfacing between blockchain and non-blockchain systems. The magnitude of this problem can be understood by the fact, that a service provider has to migrate all of its hospitals to the blockchain system simultaneously, or risk non-cooperation among its own service points. Secondly, if all cooperating service providers migrate to blockchain solutions, they may still face unification issues. Figure 3 shows three types of solutions in this regard. In the first Unified blockchain solution, all e-healthcare service providers connect to a single blockchain, which is maintained by either a consortium or by the government. Additionally, all eHS maintain their independent local servers and only send trades that involve multiple eHS. This can be viewed as a hybrid solution, which may allow some eHS to operate a traditional system, with an interface for blockchain backbone. The other systems shown in Figure 3 form a multiple-blockchain solution, where each service provider has an independent blockchain, which is then connected to other blockchains for interoperability. Here, either the eHS can make their whole peer network as part of the unified chain, or restrict some of the peers to be part of global chain while the others remain local to the chain. This is a more complex solution, but also allows individual eHS to have their independent blockchain. Here, the solutions for traditional system to blockchain interfacing is an important design issue. In any of the above mentioned solutions, the following challenges must be addressed.

### Interoperability

This allows one eHS to exchange data with another eHS without interpreting the data. It leads to increased patient engagement, easier access, boosts efficiency, and to some extent enables regulatory compliance. From an engineering perspective interoperability can be classified as:

**Structural Interoperability:** Allows the exchange of data, and either of the systems does not need to change the format of the data. It is stored and used without any interpretation.

**Semantic Interoperability:** Allows the data to be understood by the systems without any modification. This means that not only the structure of data is the same, but its meaning is also the same. For example, temperature stored as an integer but understood in Celsius or Fahrenheit.

It is also important to note that EHR interoperability standards such as Fast Healthcare Interoperability Resources (FHIR) [18], are mainly implemented at the application level. The storage of EHR is usually different due to storage and query optimization issues. However, efforts can be made to store EHRs in native FHIR format as part of the trades, which may lead to improved interoperability.

### Trade Structure

Although business blockchains allow unstructured data, the block and trade structure are fixed. For example, Hyperledger based blockchain has a block header, transaction payload, and metadata as part of the block. Each component has several parameters that represent unique information of a trade. This format may not be compatible with other protocols (e.g Ethereum). To ensure cooperation, all eHS must be able to follow the same trade format, which is difficult. A solution to this can be in Type-Length-Value (TLV) fields where each part of a block is represented by a TLV. Moreover, if all participating systems agree on the

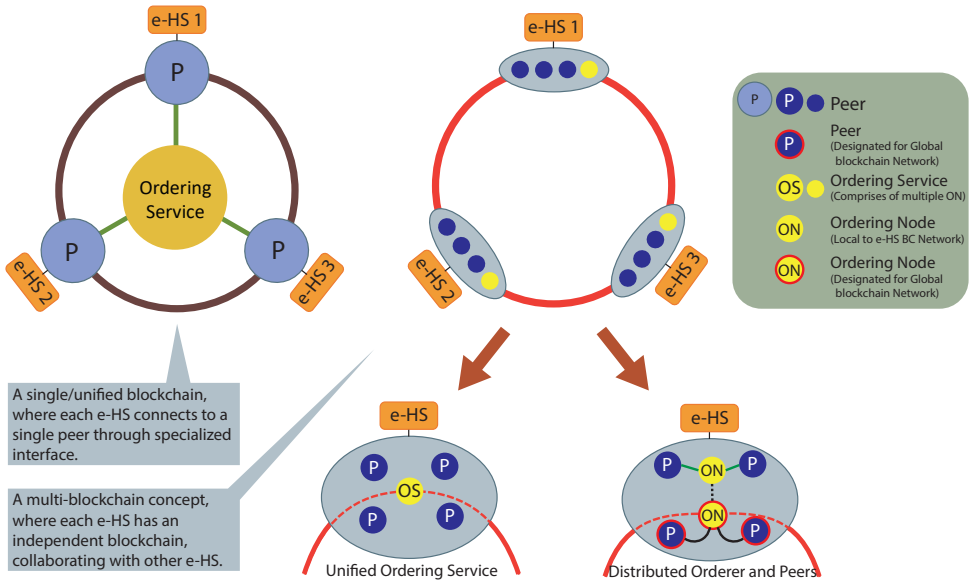


Fig. 3: Interoperability Solutions for Cooperative e-Healthcare systems.

minimum required TLVs in a block, then their order or extra TLVs will not matter. This can be an interesting research direction, as the TLV use can also enable FHIR native format for EHR exchange among different partners.

### Storage of Ledger

Once the block is formed after consensus, the ordering service sends it to all peers, which adds it to their ledgers and update the world state. This is the final commit process of BBC [19].

Sharing of a block with all peers is an interesting issue, especially if a multiple-blockchain solution is being used. Assume that two eHS are involved in a trade, which is going to be part of block $B_1$. In a unified blockchain, $B_1$ after consensus formation has to be sent to all peers. The number of trades generated by each eHS can be very large, hence the memory requirements of the ledger could be astronomically high. Efficient storage solutions become an interesting research area for this problem. On the other hand, if a multiple-blockchain solution is adopted, then the participating eHS may choose to store $B_1$ in their own peers only. This will limit the replication of block but may create access issues if the same patient visits a third eHS that requires the information stored in $B_1$. Figure 4 shows the memory required by Hyperledger Fabric at every peer. This requires an efficient trade/block discovery mechanism across different cooperating blockchain, in addition to the strict access control mechanism.

## Consensus Formation

The fundamental questions in blockchain for non-cryptocurrency applications are related to trade verification & consensus formation, and perhaps this is the most misguided research area. In a non-crypto system such as healthcare, the exchange of digital assets is the trade. Hence, any consensus has to be formed for the valid exchange of data elements.

### What to verify?

In an e-healthcare system, several IoT devices generate data related to patients which need to be stored and accessed by different service providers (such as, doctors & nurses), as well as by third-party services (insurance agencies). Similarly, a medical test report or a prescription written by a physician is also considered a digital asset. As soon as such a digital asset is created, it has to verify its validity, authenticity, and access level. Trade structure again becomes an open research challenge here.

Similarly, there can be many other events that need tracking, for example, administering a drug, which must be recorded as a trade. Requesting patients old EMR is also a trackable event. Although this does not generate digital asset, it is based on proper access control, hence a query trade must be done for this purpose.

The challenge is to identify the various types of trades that may occur in a blockchain for modern automated e-healthcare systems. In addition, the trade structure must be flexible enough for storing such dynamic information.

### How to Verify?

The process of verification begins with the smart contract and ends with block creation. Smart contracts are pre-defined agreements between any two parties willing to participate in a trade and dictates the terms of exchange.

In the given scenario, the simplest SC will exist between a temperature sensor (as an IoT device) and a patient monitoring system (as a software entity). In a more complex scenario, a patient can create an SC to grant the physician (or group of physicians) access their EMR. Similarly, a separate SC should be created with different access privileges for other medical staff. For example, a nurse may only have rights to read part of EMR and prescription information, while the physician can update all records. The challenge in this part is to enable the system to efficiently generate a diverse range of smart contracts. Many of these can be generated using predefined templates, however, creating

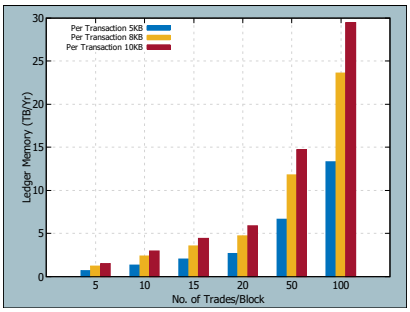


Fig. 4: Increase in Ledger memory requirement.

or changing must ensure Byzantine Fault Tolerance (BFT), which means that 51% of peers must agree to it. Scalability and ease of creation are the key points in this research challenge.

The next step is of consensus formation, which results in block formation. It ideally should have two parts, however, to improve the transaction rate (TPS), some systems only perform one. The first one is to verify the validity of each trade, which means that the trade should satisfy the associated SC, must have valid signatures of all parties, and endorsed by the peers. In the second part, the candidate block must be verified for valid signatures and endorsed by the peers. As performing both parts is time-consuming, hence the challenge is to have consensus forming protocols that are highly efficient and do not compromise on the two-part process.

It is also interesting to note that Hyperledger Fabric only performs trade verification, and does not require 51% of peers to vote. The participating peers can be as less as two. This significantly improves TPS but also compromises on BFT. However, Hyperledger fabric also allows plug-able consensus protocols, which make it a flexible platform. This opens the research direction of replaceable or dynamically changeable algorithms, where peers can decide which algorithms fit best for consensus for specific types of trades or blocks. Hence, in the multiple-blockchain solutions, different blockchains participating in a trade must either follow the same consensus formation protocol (which is too restrictive), or dynamically select one (which should be interoperable). The consensus algorithm itself should be highly scalable to work at a multiple-chain level. Similarly, smart contracts should be acceptable across different blockchain platforms, which is highly complex research challenge.

## Users & Access Control

In a public blockchain, especially for crypto-currencies, all users are created equal. They can generate transactions, or become peers for consensus formation. However, this is not the case in healthcare systems, where strict access control is required. It is important to understand the difference between access to the overall system, and access to the blockchain. In the former, the user may just be locally logged in through verification of a local certificate authority (CA) or Access Control List (ACL), but in the latter, the user can generate trades or query the ledger. The specific challenges in this area are addressed below.

### User Diversity

E-healthcare blockchain is a specialized scenario where the user type diversity is very high. This variation in type is due to their access privileges [20]. A patient has full access to all its trades (i.e. medical history), while the guardian of minor may have limited access. This may change over time, and hence the system has to adapt. Similarly, one physician may have complete access to update, while a consulting physician may only have read access, while the pharmacy may only be able to view prescription trades for a patient.

A blockchain solution by default does not address user diversification, hence it has to be tightly coupled with the ACL of the overall system. This tight coupling is an open research area. Moreover, this coupling should be highly scalable, especially in a unified blockchain environment.

### Access control & Channel Management

The coupling described earlier is a complicated solution as it requires every trade to first be cross-checked by the ACL, and hence defeats the purpose of using blockchain. A better solution is to rely on smart contracts and channels. The concept of channels initially comes from Hyperledger Fabric, where each user/device is assigned a logical path for connecting to a peer. The solution to access control can then be implemented using these paths (channel). The channel should be bound to the patient and may have different versions. Whenever the patient wants to change the access rights, a new version is created. The channel information is stored as part of the blockchain network, hence it does not rely on the ACL. Furthermore, the smart contract and channels have different responsibilities, and should be utilized efficiently.

This is still an open research challenge, however, the solution has to be managed within the blockchain network.

## Big Data

In a blockchain, the storage of information or digital asset exchange is done through transactions, where all relevant data (images, etc.) should be part of the transaction. The transactions (in the form of blocks) are stored in a file-based ledger, which cannot store large images. The typical size of a single block in any blockchain system is limited to a few megabytes, as it directly impacts the performance of the system.

E-healthcare systems are heavily dependent on medical imagery (x-rays, CT Scans, etc.) as described earlier. This reason alone may make a blockchain implementation impractical in e-healthcare systems. The solution can be found in off-chain storage, but this requires several modifications in the way trades are done, and data is stored. First, the off-chain storage should not allow any access other than which is authorized by the peer or the ordering service. As the objective of a distributed ledger was to have replicated immutable copies of data, hence off-chain storage must ensure immutability, distributed nature, and access by verified users only. Hence, this demands protocol changes for query trades. Secondly, to add data to the off-chain storage and relate it to a specific trade, the trade must contain a pointer to its storage location. This pointer can be to a hash value or

some other efficient mechanism within the storage. Thirdly, the security of off-chain storage should be assured. Just like a CA is assumed to be secure and trusted, hence practical guarantees for storage should be ensured.

All these requirements become design level challenges for blockchain implementations in e-healthcare (and big data) scenarios. An interesting idea is to consider Blockchain as a Shell around the existing and traditional database structures. This will essentially enable the use of storage & query efficiency of database systems while securing them within the working principle of a blockchain system.

## Completing the Ecosystem

Finally, EHR management is not the only process in a healthcare facility. Many other departments such as accounting, human resources, pharmaceutical logistics, emergency services, etc. are integrated into the ecosystem. As described earlier, migrating one to the blockchain will create a significant impact on inter-department communication. Most research in BC for healthcare is focused on EHRs, however, the elements and their interaction as shown in Fig. 2 is extremely important. A viable and deployable BC solution will only work if all entities in the ecosystem are in sync. Hence, the research community needs to work on BC and non-BC system interfacing, while ensuring that one does not compromise the other.

## Conclusion

The objectives of this article were to enable the reader in understanding the complexity of implementing a blockchain solution for e-healthcare systems, and look for possible solutions. Healthcare is not an isolated network, hence the blockchain solutions implemented by individual health service providers must be inter-operable, which will require new protocols for trade and consensus management. Big data management and security in off-chain storage must be an integral part of the ecosystem. Finally, blockchain is an exciting and efficient solution for many security and accountability challenged, however, migration of existing systems has a long road ahead, and the first step is to understand the needs of the application domain. Many of the design questions raised in this article may also be appropriate for other domains.

## Acknowledgments

This work is partially supported by National Natural Science Foundation of China N. 61772077, 61370192, and Beijing Natural Science Foundation No. 4192051. Drs. Sharif & Li are co-corresponding authors.

## References

[1] H. Jin, Y. Luo *et al.*, "A review of secure and privacy-preserving medical data sharing," *IEEE Access*, vol. 7, pp. 61 656–61 669, 2019.

[2] T. McGhin, K.-K. R. Choo *et al.*, "Blockchain in healthcare applications: Research challenges and opportunities," *Journal of Network and Computer Applications*, vol. 135, pp. 62–75, 2019.

[3] D. C. Nguyen, P. N. Pathirana *et al.*, "Blockchain for secure ehrs sharing of mobile cloud based e-health systems," *IEEE Access*, vol. 7, pp. 66 792–66 806, 2019.

[4] W. Mougayar, *The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology*. Wiley, 2016.

[5] P. Tasca and C. J. Tessone, "A taxonomy of blockchain technologies: Principles of identification and classification," *Ledger*, vol. 4, Feb 2019.

[6] S. Biswas, K. Sharif *et al.*, "PoBT: A lightweight consensus algorithm for scalable IoT business blockchain," *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 2343–2355, Mar 2020.

[7] Hyperledger: Hyperledger business blockchain technology. [Online]. Available: https://www.hyperledger.org/projects

[8] P. Sundaravadivel, E. Kougianos *et al.*, "Everything you wanted to know about smart health care," *IEEE Consumer Electronics Magazine*, vol. 7, no. 1, pp. 18–28, Jan 2018.

[9] S. Allen, "2020 global health care outlook," 2019. [Online]. Available: https://www2.deloitte.com/global/en/insights.html

[10] P. Pace, G. Aloi *et al.*, "An edge-based architecture to support efficient applications for healthcare industry 4.0," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 1, pp. 481–489, Jan 2019.

[11] N. Kshetri, "Blockchain and electronic healthcare records [cybertrust]," *Computer*, vol. 51, no. 12, pp. 59–63, Dec 2018.

[12] A. Azaria, A. Ekblaw *et al.*, "Medrec: Using blockchain for medical data access and permission management," in *International Conference on Open and Big Data*, Aug 2016, pp. 25–30.

[13] R. Jayaraman, K. Salah *et al.*, "Improving opportunities in healthcare supply chain processes via the internet of things and blockchain technology," *International Journal of Healthcare Information Systems and Informatics*, vol. 14, pp. 49–65, Feb 2019.

[14] V. P. Yanambaka, S. P. Mohanty *et al.*, "PMsec: Physical unclonable function-based robust and lightweight authentication in the internet of medical things," *IEEE Transactions on Consumer Electronics*, vol. 65, no. 3, pp. 388–397, Aug 2019.

[15] A. D. Dwivedi, G. Srivastava *et al.*, "A decentralized privacy-preserving healthcare blockchain for iot," *Sensors*, vol. 19, no. 2, 2019.

[16] Health Insurance Portability and Accountability. [Online]. Available: https://hhs.gov/hipaa/

[17] General Data Protection Regulation. [Online]. Available: https://gdpr-info.eu

[18] Fast Healthcare Interoperability Resources (FHIR) R4. [Online]. Available: https://www.hl7.org/fhir/

[19] S. Biswas, K. Sharif *et al.*, "A Scalable Blockchain Framework for Secure Transactions in IoT," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4650–4659, June 2019.

[20] W. Zhang, Y. Lin *et al.*, "Inference attack-resistant e-healthcare cloud system with fine-grained access control," *IEEE Transactions on Services Computing*, pp. 1–1, 2019.

## Biographies

**Sujit Biswas** received his Ph.D. degree in Computer Science and Technology from Beijing Institute of Technology, China. He is an assistant professor with Computer Science and Engineering department, Faridpur Engineering College, University of Dhaka, Bangladesh. His basic research interest is in IoT, Blockchain, Mobile computing security and privacy, Big Data, Machine Learning, Data driven decision making, etc. Contact him at sujitedu@bit.edu.cn.

**Kashif Sharif** is an associate research professor with the Beijing Institute of Technology, Beijing, China. He holds a Ph.D. in Computing and Informatics from University of North Carolina at Charlotte, NC, USA. His research interests include Wireless communication, Blockchain & DLTs, Programmable networks, and Data centric networks. He is an AE of IEEE Access. Contact him at kashif@bit.edu.cn.

**Fan Li** is a professor with with the Beijing Institute of Technology, Beijing, China. She holds a Ph.D. in Computer Science from University of North Carolina at Charlotte, NC, USA. Her research interests include wireless networks, ad hoc and sensor networks, and mobile computing. Contact her at fli@bit.edu.cn.

**Saraju P. Mohanty** is the Editor in Chief of the IEEE Consumer Electronics Magazine and Professor in the Department of Computer Science and Engineering (CSE), University of North Texas (UNT), Denton, TX, USA. His research is in "Smart Electronic Systems" which has been funded by many agencies including the National Science Foundation, the Semiconductor Research Corporation, the US Air Force, the IUSSTF, and the Mission Innovation. Contact him at saraju.mohanty@unt.edu.