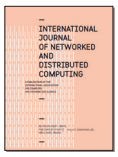
International Journal of Networked and Distributed Computing
Vol. 7(4); September (2019), *pp.* 158–166
DOI: https://doi.org/10.2991/ijndc.k.190917.001; ISSN 2211-7938; eISSN 2211-7946
https://www.atlantis-press.com/journals/ijndc



Research Article

A Secure and Scalable Data Source for Emergency Medical Care using Blockchain Technology

Shirin Hasavari*, Yeong-Tae Song

Department of Computer and Information Science, Towson University, 7800 York Road, Towson, MD 21117, USA

ARTICLE INFO

Article History

Received 25 March 2019
Accepted 10 May 2019

Keywords

Permissioned blockchain network
emergency medical care
scalable blockchain

ABSTRACT

A relationship exists between the emergency patient death rate and factors such as the failure to access a patient's critical data and the time it takes to arrive at hospitals. The ability for Paramedics to access a patient's complete picture of emergency-relevant medical data is critical and can significantly reduce the annual mortality rate. Today, the problem exists with a continuous recording system of the patient data between healthcare providers. In this paper, we have introduced a blockchain-based solution to record patient emergency relevant medical data as patient walks through from one medical facility to another, creating a continuous footprint of patient as a secure and scalable data source. Therefore, ambulance crews can access and use it to provide high quality pre-hospital care.

© 2019 *The Authors*. Published by Atlantis Press SARL.
This is an open access article distributed under the CC BY-NC 4.0 license (http://creativecommons.org/licenses/by-nc/4.0/).

1. INTRODUCTION

In a medical emergency, prior knowledge of a patient medical record can make a difference especially in life or death situation. However, with current medical record setting, it is difficult to access a patient's medical history as caregivers who treat the patient in emergency do not know where the patient emergency data is located and even if they know where they are, they may not have access to the relevant medical records. There have been many attempts to resolve the issue, but no comprehensive solution exists as some healthcare providers use trusted third-party solution to communicate and share patient data while others prefer to use cloud-based medical data storage and sharing. Among others, there has been an approach to use blockchain network as a medical data-record management platform. In our approach, we use blockchain technology as a potential solution for emergency medical data management.

It is naive to think that the healthcare industry will discard today's solutions and re-implement its record keeping systems on a blockchain architecture. Healthcare exists as a risk-adverse industry, unlikely to readily accept the time and cost required to shift to a new and unproven technology. To achieve high rates of Electronic Health Records (EHR) adoption, the Centers for Medicare & Medicaid Services have spent over US$30 billion since 2011 [1]. A new approach for record keeping will need to respect this investment and work alongside the existing platform, not supplant it. The institutions maintaining healthcare data in centralized systems perceive patient data as a valuable asset, making it difficult to change their way of thinking. While a blockchain-based solution may be a full alternative option at some point in the future, the near-term requires building a bridge to the blockchain platform. That is why our solution will use the secure file transfer tools/protocols as a bridge to reach the blockchain.

Furthermore, this combination includes some innovative ideas to reduce some concerns surrounding blockchain usage like scalability or uncertainty about its adoption in the medical field, especially emergency medical services that utilize emergency medical data which consists of current problems, allergies, medications and demographic information.

Today, some medical facilities use file transfer tools to send patients' medication codes to insurance companies. Some regulatory bodies such as the Department of Health and Human Services may decide when and how to access or share the data. Therefore, they are familiar how to use these tools.

In this approach, we are going to introduce a solution to touch some major issues like fragmenting medical data, accessing the data using an intermediary. We are also going to provide a suggestion on how to handle data scalability that is an ongoing debate on applying blockchain to healthcare domain.

2. BLOCKCHAIN TECHNOLOGY

Blockchain is a technology that has designed to focus on streamlining the appropriate flow of information in business networks and to ensure that we can share the information that need to be shared very easily and very rapidly in a manner that minimizes the amount of time that people have to finding and correlating information across business networks.

It is a comprehensive application of computer technology, which combines encryption algorithm, P2P network, distributed storage, consensus algorithm and smart contracts. The blockchain technology

*Corresponding author. Email: Shasav1@students.towson.edu

is a decentralized, transparent, traceable, and resistant platform but still is further developed to be applied in more fields.

It can maintain unmodifiable and continuously growing data records. Transaction is an important concept in blockchain, a special database where transactions can be added to but not deleted, and all the operations are recorded as transactions. The basic data structure of blockchain exists as a linear linked list, linked with blocks and each block contains information such as the hash of pre-block, the hash and address of the block, the information of transactions and other useful information. New transactions should be added into a new block. All the nodes should reach an agreement on the transactions by consensus algorithm and then added to the blockchain. All the nodes can check the validity of blocks by computing hash with a blockchain being executed in a distributed peer-to-peer network. Nodes in the blockchain network can interact with each other without needing a trusted intermediary [2–6].

2.1. Selection of Blockchain Framework

Many frameworks for blockchain technology exist and depending on the participants, blockchain gets divided into public chain or to the private chain. Only members of one institution can have access to the private chain. Consortium chains can be jointly maintained and used by several institutions. Bitcoin, Ethereum and Hyperledger Fabric are the most popular frameworks. Bitcoin and Ethereum belong to public chain and versions of permissioned Ethereum are available. Hyperledger Fabric is the private/permissioned model. We have chosen the Hyperledger Fabric for the following requirements.

- Not reliance on intermediaries or third parties for data validation and access such as Health Information Service Providers (HISPs).
- Data is replicated and distributed among participants, hence a common view of the same transaction/data.
- Privacy and confidentiality of transactions through implementations of channels which is a subnet of network that all members can privately distribute and share their data.
- Data is immutable which means that no updates or deletes occurs in place. Updates and deletes are added to the previous ones indicating new state. Hence, highly data breach/fraud resilient.
- Participants must be identified/identifiable—and invited, hence permissioned.
- Writes and read permissions are role-based and usually requires consensus of several participants.
- Multiple algorithms are used for consensus and each organization can create a customized consensus based on their unique requirements.
- Modular and highly configurable architecture.
- Improve auditability.

Figure 1 depicts the Hyperledger Fabric platform.

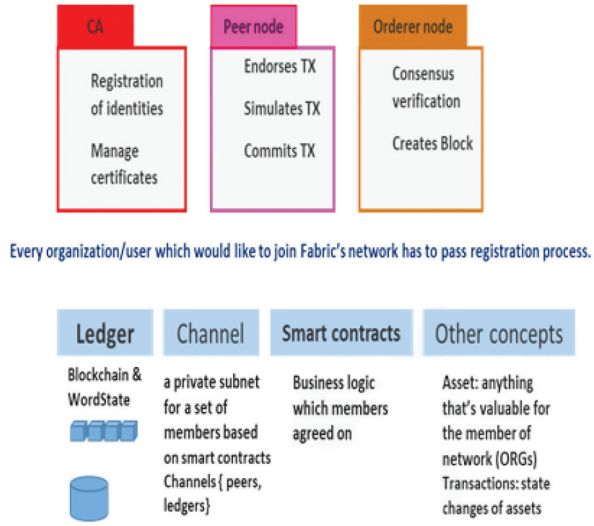


Figure 1 | Hyperledger Fabric components.

2.1.1. Components functionality

The components of this platform cooperate to meet the cross-organizational requirements. Hyperledger Fabric network requires any healthcare provider or medical facility, which is going to transfer their data to the network to go through the process of registering with a trusted identity and enrolling to get access to network resources. The following statements help us to understand these components individual and mutual functionalities [7].

- **The Fabric-CA component**: Each participant registers with proof of identity to the network membership services to gain access to the network resources.
- **Membership Service Provider**: Provides services for managing identity, privacy, confidentiality and auditability on the network. All components use Membership Service Provider to authenticate each other mutually to communicate and share resources.
- **Peer node**: The blockchain network is built up from the peers owned and contributed by the different organizations. A node can join the blockchain network as performing one or more functionality related with endorsers, orderers and validators and committers.
- **Endorsing node**: Will simulate and sign or reject the transactions. It creates a read/write set of the asset on which a transaction has been requested. A transaction is a request to read or write on the ledger. New transactions are appended to the blockchain as a new block and world state database is updated to reflect the new state.
- **Orderer or ordering peer:** Runs the consensus algorithm on the transactions and order these transactions appropriately in a block based on their channel ID. It sends the blocks of transactions to validating/leading peers.
- **Validating peer:** Checks transactions against endorsement policy (i.e. *n* out of *m* endorsing peers need to simulate and sign the transaction before it hands out to the orderer). It also performs version control to ensure there is identical R/W () sets for all peers. Then it sends the transaction to the committing peers.

- **Committing peer:** Receive the block of transactions from validating/leading peer and appends it to the blocks and update their respective database (level DB or CouchDB).
- **Ledger:** Consists of two distinct, though related parts—blockchain and a word state database. A blockchain is an immutable sequence of blocks, each of which contains a set of ordered transactions. A world-state is a database that holds the current values of a set of ledger states.
- **Channel:** A subset of the Fabric network through which peers interact with each other, and with applications—a mechanism by which these components within a blockchain network can communicate and transact privately.
- **Smart contract:** Defines the executable logic that generates new facts that are added to the ledger.

For better grasping the inter-functionality concept between these components, the Figure 2 depicts a transaction-flow sequence diagram in the Hyperledger Fabric network.

To make the sequence diagram more precise, we did not include failure points or false conditions in the network. Figure 3 depicts a

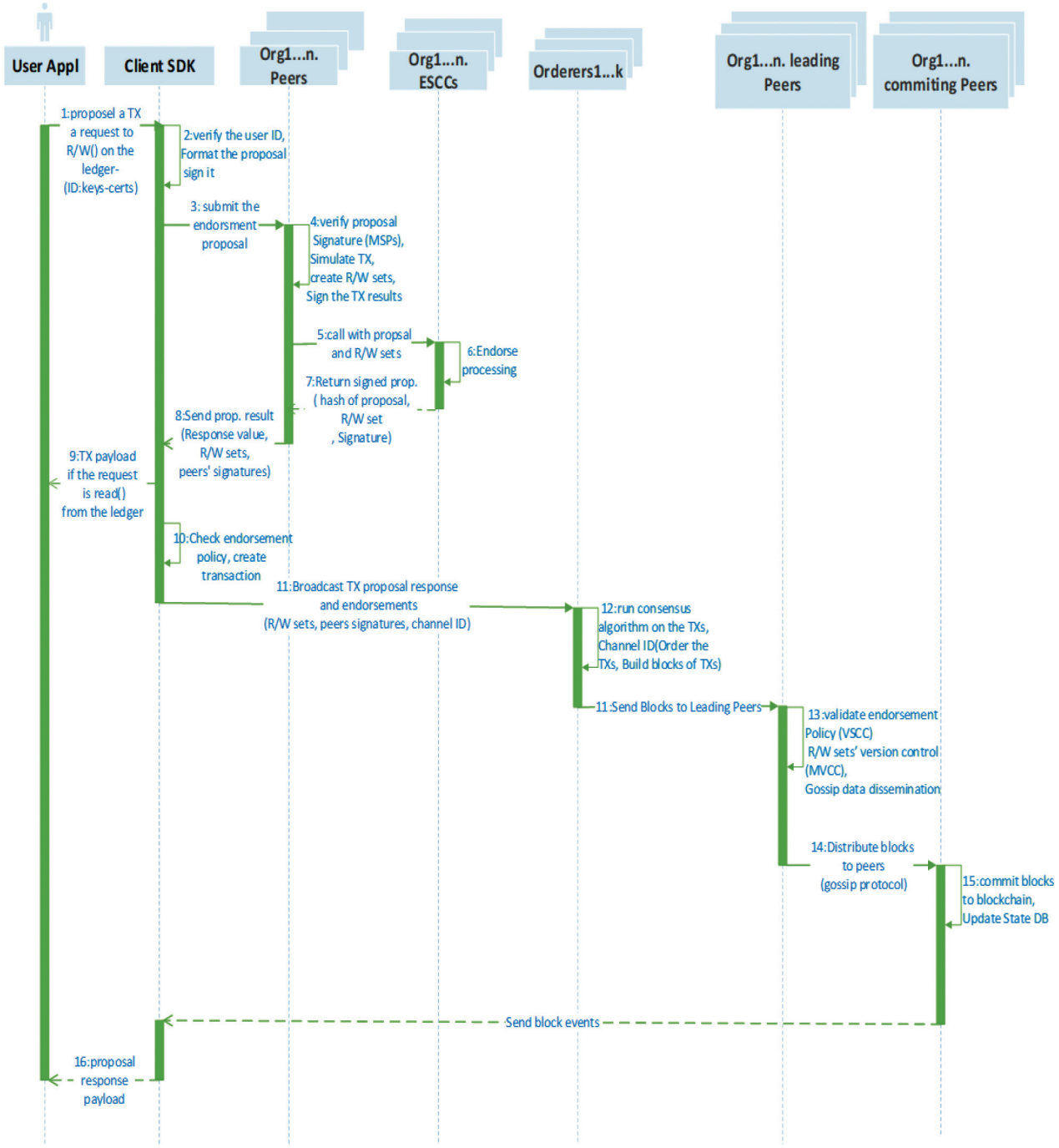


Figure 2 | Transaction-flow in Hyperledger Fabric.

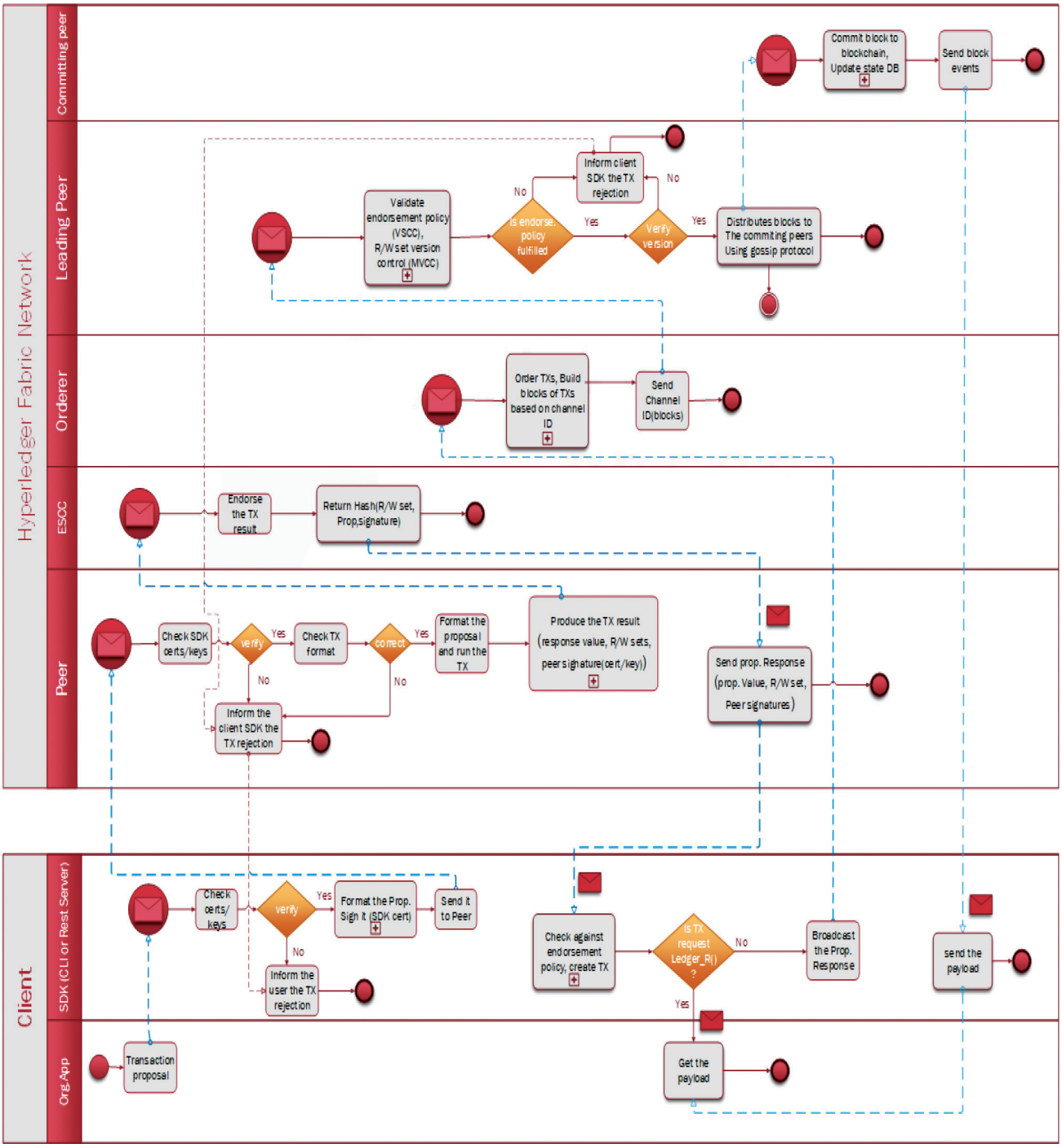


Figure 3 | BPMN of Hyperledger Fabric.

Business Process Model and notation (BPMN) diagram, which presents a different view of the transaction flow through the network.

3. RELATED WORK

Envisioned as regional networks, Health Information Exchange Service Providers (HIEs) connect the many disparate entities interacting with patient data relevant to a patient's condition. Unfortunately, Emergency Medical Services (EMS) has been involved in only a few HIEs nationally, either because of a lack of funding, technology or collaboration [8,9]. Another inefficiency with HIEs is that it is an intermediary for sharing data of any kind. It is not cost effective and it also would not come up with a holistic view the way blockchain does. Another approach is EMS HIE Integration, which uses Search, Alert, File, Reconcile system to aid EMS providers in Health data exchange to follow the same conceptual and technical solution as with HISPs [10].

One solution suggests replacing EMS patient care reports with electronic health records enabling them to interoperate with other EHRs. Although, this seems a successful approach as some EHRs

connect to each other and can communicate patient medical and clinical information, a big part of the problem is exactly how many EHR versions exist and the average number of platforms hospitals run. Studies show that achieving interoperability among different EHR platforms is very difficult [11].

A decentralized record management system to handle electronic health records, MedRec uses Blockchain technology to manage authentication, confidentiality, accountability and data sharing. The platform utilizes Ethereum's smart contracts to create the intelligent representations of existing medical records to store them within individual nodes on the network. So, more hashed pointers of medical records get stored on the blockchain than the raw data itself [12]. MedRec is a record management system focusing on Electronic Medical Records (EMRs) using smart contract but raises privacy concerns [13].

Another solution suggests integrating the Hyperledger platform with InterPlanetary File System Protocol (IPFS), a peer-to-peer method of storing and sharing media in a distributed file system, not a blockchain, and this peer-to-peer file sharing system uses BitTorrent technology [14]. The data itself gets stored on the ISPF and its hash pointer on the blockchain. Therefore, we need two platform to store and distribute data so it would cause delay to access data in emergent situation. Additionally, it brings additional technical and economic burdens on the client side. The Majority of Current solutions for medical data sharing and distribution using permissioned blockchain technology to rely on business process integration which clients runs codes on each node to go through certain processes until they store the data on the ledger. This approach requires excessive work on the Hyperledger client side. To solve this problem, we need to extract the Emergency Medical data (EMS) generated by a health care provider in place and transfer it, indicating that the processes which have generated the medical data have finished.

4. OUR APPROACH

Health care settings and providers are reluctant to share their medical data sources as a connection point to the external systems due to security issues. So, they prefer to create files and transfer them to the other systems using well-known tools with which they are familiar. To reduce the workload on the client side the solution offers a combination of Secure File Transfer Protocol (FTPS) to securely transfer file and blockchain as an ultimate source of data.

Health Insurance Portability and Accountability Act (HIPPA) requires encryption for privacy and security so we encrypt our data with Transport Layer Security (TLS) between client (clinic/medical facility) and servers (peer node on the Fabric network).

The permissioned blockchain working on a pre-defined consensus and business logic, demands strong identity management, accountability, access control, and authorization. Before transferring data, the health care provider needs to obtain an enrollment and transaction certificate to connect to and access the resources on the Fabric network. Eligible healthcare providers can use their own digital certificate (X.509) as a trusted identity.

Figure 4 and the following statements explain the process.

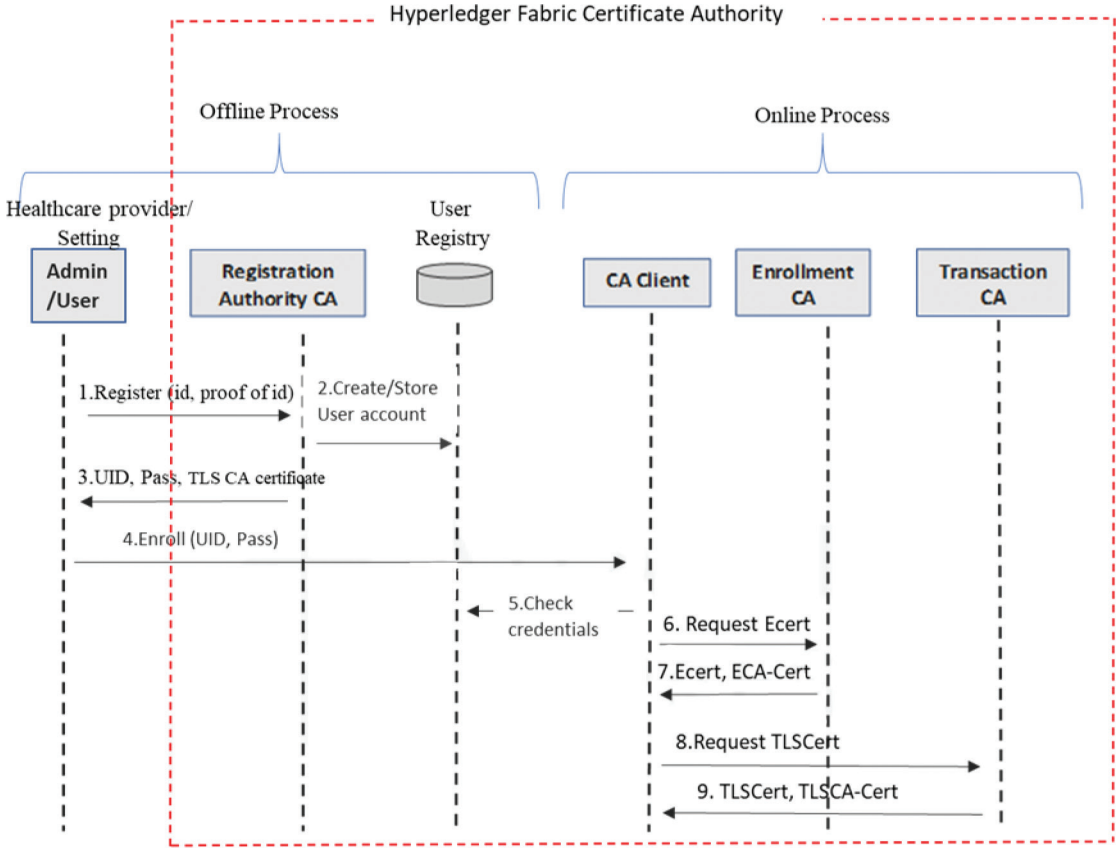


Figure 4 | Member registration and enrollment, getting certificates.

4.1. Registration and Enrollment Process

- **Registration authority**: Validates identity/role and issues registration credentials to enroll with Enrollment Certificate Authority (ECA).
- **Registration Certificate Authority = Registration Authority itself (RCA)**: Creates and stores admin/user account in user registry data source like Lightweight Access Directory Protocol (LDAP) and assigns an ECA-Cert to the CA-client and sends it to the admin/user so that admin/user can interact with CA-client as a trusted anchor. RCA also issues User Identification (UID) and Password and a Transaction Certificate to the admin/user.
- **Admin/user**: Uses UID and Pass to the CA-client so that CA-client accept it as a trusted actor and interact with Enrollment-CA and Transaction-CA on behalf of the user to enroll admin/user and to issue the necessary certificates to the admin/user so the admin/user can connect and have access to the Fabric resources.
- **CA-client**: Check the admin/user and verify it. Then, it is ready to interact with Fabric-CA on behalf of the user. It, on behalf of the user, sends a request to Enrollment-CA to receive an Enrollment Certificate (ECert).
- **Enrollment Certificate Authority**: Issues ECert to admin/user after validating the registration credentials. ECA also issues its own ECA-Cert to the CA-client so that CA-client send it to the Transaction-CA to prove that it has gotten the ECert from a trusted source (Enrollment-CA).
- **CA-client**: Sends a request to Transaction-CA to get TLS-Cert to submit transactions to the network and Transaction-CA finally issues a TLS-Cert to CA-client and its own TLSCA-Cert.

After the registration and enrollment processes the healthcare provider get the necessary certificates to connect to, access and use the Fabric network resources (peers, channels, ledgers, etc.).

As highlighted above our solution involves the use of a FTPS file transfer protocol using an advanced tool to schedule and automate the secure uploading of the patient emergency relevant to the medical data on a TLS server residing on the Fabric blockchain. A Peer node needs to be configured as a TLS Server to receive the data and place it on a shared folder. A data format standard may apply to the receiving of data either before or after the uploading to make the data consistent and identifiable. Then a TLS server needs to communicate with the ordering node which builds the blocks of data and distribute it among the other nodes. Nodes will validate the data and will commit it to their ledger.

To reach a consensus, ordering nodes representing the members of a subnet/channel need to follow strict algorithms. After the data is stored on the ledger a previously scheduled task can remove the data from the shared folder to prevent scalability issues in the shared folder.

Scalability on the ledgers can be controlled in a way that whenever a patient's EMR data gets updated by a healthcare provider then it can be transferred to the TLS server on the Fabric network. In TLS communication, the client application needs to provide its X.509 certificate as a trusted identity to the TLS server so that no malicious third party can upload a fake medical data on the TLS server.

After exchanging certificates, everything gets performed inside the Fabric network and the peer node configured as a TLS server needs to get configured as a TLS client too to be eligible to request resources inside the network. The TLS Server node acts as the TLS client now to send transactions to the ordering node which performs the access control against the TLS client to validate the request, ordering the transactions, building the blocks of data and distributing them to the validating peers residing on the subnet. Validating peers need to verify the modifications approved by the ordering nodes indeed satisfying the policies defined in the subnet/channel. After blocks get added to the ledger on each organization's peer, a notification gets sent to the original client. Figure 5 depicts the process.

Figure 6 depicts a sequence diagram of our approach.

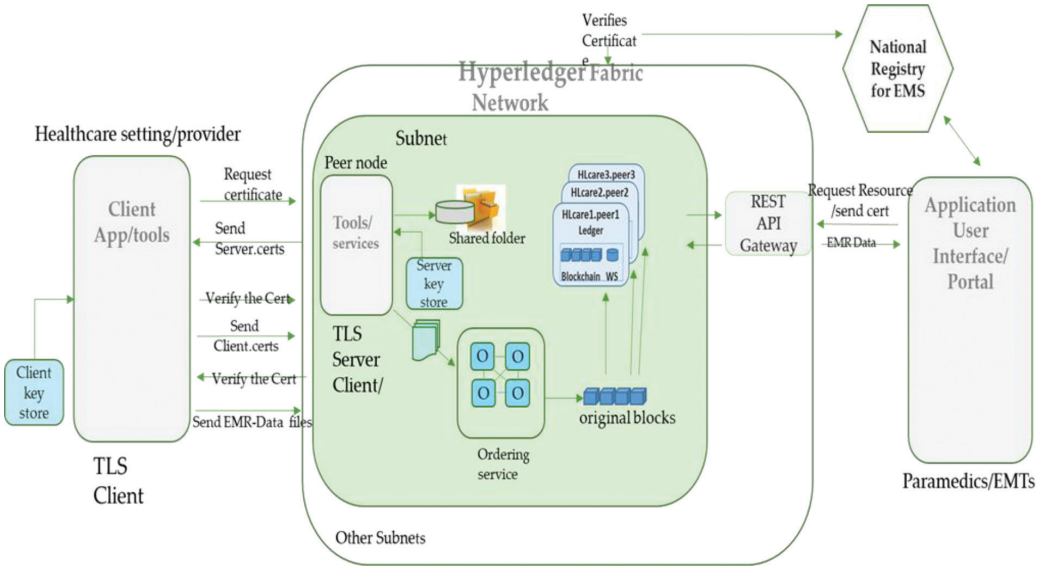


Figure 5 | Emergency-relevant medical data recording and access on the blockchain.

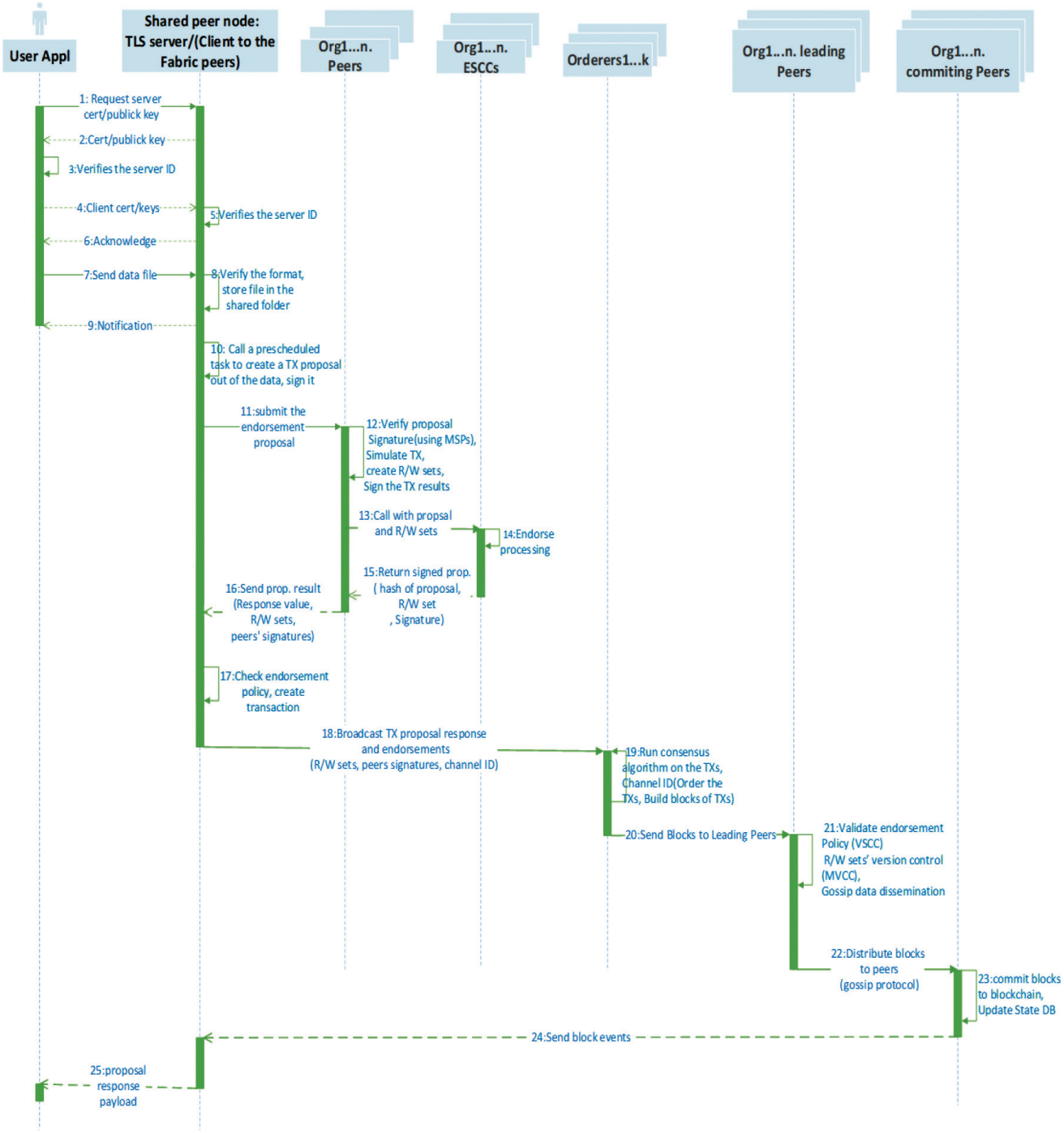


Figure 6 | Data flow sequence diagram of our approach between clients and Hyperledger Fabric network.

As shown in the picture our approach keeps the end-user client/organization platform as less as busy, so much of the work is performed in the Fabric platform once organization transfer the data and get the confirmation.

The latest version of the Hyperledger Fabric works based on execute-order-validate to avoid non-deterministic chaincode. In the non-deterministic chaincode whatever R/W() sets that a specific channel's validating peers produce may not be identical, so this cannot be appended to the blockchain as each peer can have different version of the same (key, value) pairs which is not the goal of this platform. That is why we have the endorsing nodes to simulate the data and store the read() version temporarily. In the next step, when leader peers or validating peers read the data from state DB, they can compare it and do version control. They will send the result to commit peers once to ensure there is identical R/W() sets for all peers. In our approach we have followed the same consensus solution.

We may develop a customized consensus solution to keep the interaction across the network short to save the time. Hyperledger Fabric is an open source platform allow developers to customize it based on the organizations' unique requirements.

5. DATA STANDARDS

For taking care of semantic aspect of medical data stored on the ledger, we can follow the existing data standards. For example, the International Statistical Classification of Diseases and Heath Related Problems (ICD-10) for diseases and RxNorm for medications or prescribed drugs. When committing data, these codes along with their names can be stored on the ledger. This data later can be used for communicating with insurance entities as well.

6. PATIENT IDENTITY ON THE LEDGER

A challenging part of patient data query in any system is that how to identify a patient in a deterministic way and which attributes need to be used while requesting a certain patient data. As a matter of fact, different healthcare providers like hospitals, clinics, physician offices and other medical facilities may define and store their patients' identification in a different format. So, we need to make sure that our system provides a consistent way to record and identify a patient uniquely. A fundamental component of safe patient care is ensuring that the "right" patient receives the care that was intended. This expectation is most clearly defined in the Joint Commission's first National Patient Safety Goal [15]. Although there are strategies for improving the safety of patient's identification, but it is still probabilistic and not deterministic. In most emergency cases, patients themselves cannot be a reliable source to providing information about their medical data or even for their identity due to their extreme condition. The patient maybe unconscious or he/she is not able to remember the medications they are taking. Health technology assessment information service special report has discussed and introduced patient identification errors issues [16].

Identifying patient in emergency is not subject of our approach. It is another project in and of itself. We only deal with the part of as to how to register a patient identity in our system while recording their respective data coming from a certain medical facility and how an external application like ambulance's Electronic Patient Care Reporting System (eCPR) can query it. Current solution in Hyperledger is distributed framework for patient digital identities, which uses private and public identifiers secured through cryptography, creates a singular, more secure method of protecting patient identity. For example, in other approaches like HIE—master patient index challenges arise from the need to synchronize multiple patient identifiers between systems while securing patient privacy.

Additionally, we are going to borrow the recently developed methods of how we can look up a certain patient data across many blockchain-based networks, such as Hyperledger quilt—an implementation of the inter-ledger Protocol for inter-ledger interoperability. The objective of this initiative is the advancement of cross-industry collaboration through the development of blockchains and distributed ledgers [17].

7. PARAMEDICS ACCESS TO THE DATA SOURCE ON FABRIC NETWORK

The ambulance software application/App user may or may not be a member of the Fabric network to be eligible to access the data. If not a member, the blockchain will look up the national registry database in which the paramedic is registered with a trusted identity like X.509, to provide authentication. Client App like ePCR will be using Rest Application Programming Interface (API) to connect, authenticate and query the EMR data. The detail will be further discussed in the next paper.

8. CONCLUSION

In this paper we have proposed a solution to create a consistent, scalable and secure data source for healthcare providers such as paramedics or ER doctors to access patient's emergency clinical data for better care of the patient. In our approach, we combined FTPS-based file transfer tools and Hyperledger Fabric blockchain for creating a secure and holistic view of emergency medical data on the ledger. When patients move from one clinic/medical facility to another, their medical data can be recorded by creating a chain of blocks, which provide a consistent perspective of the patient health situation.

This way, the original data gets replicated and distributed to any other members of the network based on the policies they agreed upon. We also have proposed a simple practice to control the scalability which is currently an ongoing debate on obtaining the blockchain for the healthcare. The practice suggests that no data gets transferred and recorded on the ledger unless it has been updated by healthcare providers such as doctors or any relevant clinicians. Thus, the amount of data committed on the ledger can be reduced.

9. FUTURE WORK

In the next step we are going to create a prototype of the blockchain applications which involves creating a prototype of a blockchain network with all its components and a prototype of client-side's front-end app/tools and client's backend storage with actual or virtual patient data. All functions discussed above will be performing by this new system. Further research can be done on patient identification mechanism and find out as how to develop a deterministic patient identification among different Hyperledger Fabric networks. Indeed, participants in two or more different Hyperledger blockchain networks can transfer value between themselves using Hyperledger Quilt to achieve interoperability across the networks. It is based on inter-ledger protocol.

CONFLICTS OF INTEREST

The authors declare they have no conflicts of interest.

REFERENCES

[1] D. Ivan, Moving toward a blockchain-based method for the secure storage of patient records, HealthIT.Gov, ONC/NIST Use of Blockchain for Healthcare and Research Workshop, Gaithersburg, MD, 2016. https://www.healthit.gov/sites/default/files/9-16-drew_ivan_20160804_blockchain_for_healthcare_final.pdf (accessed February 18, 2019).

[2] M. Peck, Understanding blockchain technology: abstracting the blockchain, 2018.
[3] M. Peck, Understanding blockchain technology: the costs and benefits of decentralization, 2018.
[4] R. Chatterjee, R. Chatterjee, An overview of the emerging technology: blockchain, 2017 3rd International Conference on Computational Intelligence and Networks (CINE), IEEE, Odisha, India, 2017, pp. 126–127.
[5] M. Mettler, Blockchain technology in healthcare: the revolution starts here, 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), IEEE, Munich, Germany, 2016, pp. 1–3.
[6] Z. Zheng, S. Xie, H. Dai, X. Chen, H. Wang, An overview of blockchain technology: architecture, consensus, and future trends, 2017 IEEE International Congress on Big Data (BigData Congress), IEEE, Honolulu, HI, USA, 2017, pp. 557–564.
[7] Hyperledger Fabric. https://fabric-docs-test.readthedocs.io/en/latest/protocol-spec/.
[8] C. Williams, F. Mostashari, K. Mertz, E. Hogin, P. Atwal, From the office of the national coordinator: the strategy for advancing the exchange of health information, Health Aff. (Millwood) 31 (2012), 527–536.
[9] H. Wu, E.M. LaRue, Linking the health data system in the U.S.: challenges to the benefits, Int. J. Nurs. Sci. 4 (2017), 410–417.
[10] The Office of the National Coordinator for Health Information Technology, Emergency medical services data integration to optimize patient care, 2017.
[11] Paramedic Chief Digital Edition, Why electronic health records will replace EMS patient care reports, 2017, https://www.ems1.com/ems-products/technology/articles/why-electronic-health-records-will-replace-ems-patient-care-reports-PvRCHTjv1XXoltOR/.
[12] A. Ekblaw, A. Azaria, J.D. Halamka, A. Lippman, A case study for blockchain in healthcare: "MedRec" prototype for electronic health records and medical research data, Proceedings of IEEE Open & Big Data Conference, MIT Media Lab, 2016.
[13] X. Liang, J. Zhao, S. Shetty, J. Liu, D. Li, Integrating blockchain for data sharing and collaboration in mobile healthcare applications, 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), IEEE, Montreal, QC, Canada, 2017, pp. 1–5.
[14] E. Zaghloul, T. Li, J. Ren, An attribute-based distributed data sharing scheme, 2018 IEEE Global Communications Conference (GLOBECOM), IEEE, Abu Dhabi, United Arab Emirates, United Arab Emirates, 2018, pp. 1–6.
[15] S.F. Paparella, Accurate patient identification in the emergency department: meeting the safety challenges, J. Emerg. Nurs. 38 (2012), 364–367.
[16] ECRI Institute Health Technology Assessment and Information Service, Patient Identification Errors, 2016, https://www.ecri.org/Resources/HIT/Patient%20ID/Patient_Identification_Evidence_Based_Literature_final.pdf.
[17] M. Scott, Hyperledger's latest effort to "quilt" together blockchain networks (October 20, 2017), https://www.hyperledger.org/category/hyperledger-quilt.