Content list available at ITC

Techno-Science Research Journal

Journal Homepage: http://techno-srj.itc.edu.kh/

Techno-Science Research Journal

Decentralized Blockchain-based PKI for Patient Identification in the Blockchain Network

Vanny Ratanak Chheang[1*], Dona Valy[1,2], Dara Tith[3]

[1] *Department of Information and Communication Engineering, Institute of Technology of Cambodia, Russian Federation Blvd., P.O. Box 86, Phnom Penh, Cambodia*

[2] *Mechatronic and Informatiion Technology Research Unit, Research and Innovation Center, Institute of Technology of Cambodia, Russian Federation Blvd., P.O. Box 86, Phnom Penh, Cambodia*

[3] *Faculty of Computer Science, University of Namur, rue de Bruxelles 61, B-5000 Namur, Belgium*

Received: 29 August 2022; Accepted: 10 October 2022; Available online: June 2023

Abstract: *In the chain of the healthcare domain even in the public or private sector of a developing country, there is still much concern about information sharing, security, and privacy, especially for identity management. In Cambodia, currently, the centralized framework for identity management is mostly used, which highly depends on a single trust third-party Certificate Authority (CA) such as the General Department of ICT (GDICT) at the Ministry of Post and Telecommunication for making decisions. The identity of data is owned and managed by the service provider, so the risk might occur once the CA is hacked, the adversary could distribute false certificates with pseudo-identity. This research proposes a decentralized blockchain-based PKI for patient identification in the Blockchain network. It is decentralized, removes the need for having Certificate Authorities (CAs) and Certificate Revocation Lists (CRLs), and supports important functionalities for enrollment, verification, validation, update, and revocation of certificates. As the result, the decentralized identification model that supports the healthcare domain has been proposed in developing countries.*

Keywords: Decentralized Blockchain; Hyperledger Fabric; Public Key Infrastructure; Identification

1. INTRODUCTION

Healthcare is one of the most heavily regulated sectors in existence, mostly because of the sensitivity of the collected data such as patient medical records, patient personal records, and credit card numbers, where there is no direct contact between parties, and millions of users participate, it is necessary to identify who owns what data information and verify its source. Identification is crucial for the efficient and effective delivery of health services and public health management. However, in many countries, patient identification and information systems have been historically weak. Almost every patient goes through multiple registration processes in their lives, hospital and clinic records are often paper-based, or (where digital) have stand-alone identifier systems that cannot communicate, transfer data or records, or aggregate data between or within facilities. Many hospitals in Cambodia, mostly used the centralized framework for identity management which highly depends on trust third-party Certificate Authority (GDICT) for making decisions, and the identity of data is owned and managed by the service provider, so the risk might occur once the CA being hacked by distributing false certificates with pseudo-identity [1]. So, it is difficult to establish trusted relationships between entities.

According to McKinsey Global Institute analysis [2], a good digital identity has the following characteristics: verified and authenticated to a high degree of assurance across digital channels, unique to each individual, protects user privacy, establishes user consent, and ensures user control over personal data. Authentication is the major key to guaranteeing the identities of the data owner. Implementing identity management in healthcare facilities can lead medical professionals to enjoy a single view of identity, reduce human error, cut down costs, and improve data security.

Public Key Infrastructure (PKI) is mainly used to guarantee identities. It is an infrastructure in which a certificate authority (CA), which is a trusted third party, guarantees the relationship between an entity and a public key. It also contains a mechanism for verifying communication partners by digital signatures. In

[*] Corresponding author: Vanny Ratanak Chheang
E-mail:vannyratanakchheang@gmail.com ; Tel: +855-93 932 805

the traditional PKI, the CA has a central role and is responsible for enrolling and revoking public keys. This is what makes the PKI ecosystem fragile and prone to attacks and operational failures: several CAs have been compromised, and many fraudulent certificates were issued and used for man-in-the-middle attacks [3].

To prevent all of these issues, we propose a Decentralized Blockchain-based PKI for Patient Identification in the Blockchain Network such as (1) It is decentralized, removes the need for having Certificate Authorities (CAs) and Certificate Revocation Lists (CRLs), and supports important functionalities for enrollment, verification, validation, update, and revocation of certificates; (2) We incorporate web of trust (WoT) into blockchain-based PKI such that enrollment, verification, and validation of nodes are based on consensus between N number of nodes (numbers of pre-selected participant nodes). We deploy the practical byzantine fault tolerance algorithm PBFT as the consensus mechanism; (3) Each hospital participant is considered a member of the consensus group. Each participant must sign the agreement under governing of the Ministry of Health of Cambodia to participate in the secured channel; (4) All the certificates are validated and verified during the enrollment procedure by the consensus group.

Kakei et al. [4], the author proposed a distributed authentication infrastructure that decentralizes CA trust points so they are distributed among multiple service providers and connects them via cross-certification, a method that uses a smart contract on Hyperledger Fabric. Madala et al. [5], the author proposed a certificate transparent (CT) using blockchain that utilizes a private blockchain (Hyperledger Fabric). In their method, a CA, which is a member of the blockchain network, issues a public key certificate and stores it in a distributed ledger along with a revocation state (revoked/not revoked). The distributed ledger distributes the certificate to all peers and guarantees that it cannot be tampered with. Yakubov et al. [6], the author proposed a novel blockchain-based PKI management framework that can issue, validate and revoke X.509 standard certificates using Blockchain technology. Their framework resolves the problems with traditional PKI systems - in particular, certificate revocation, elimination of single points of failure, and rapid reaction to CAs misbehavior. They designed and developed a prototype for issuing, validating, and revoking PKI certificates through the Ethereum blockchain. Bo et al. [7], the author present a distributed blockchain-based PKI, referred to as Cecoin. In their method, distributed nodes in P2P network resemble as miners can verify the validity of certificates following a set of rules to ensure ownership consistency, and allow an identity to bind multiple public-key certificates, managing public key certificates with domain names using a decentralized certificate library based on the Merkle Patricia tree.

To sum up, the research on decentralized PKI is still in progress. The authors focus on the public (Permissionless Blockchain) and decentralized PKI system model and described a detailed scheme and the application of decentralized, PKI-based secure communication. Their designs provide the essential functions of PKIs, such as registering, updating, revoking, and verifying the ownership of a certificate. In addition, there's no research team who focuses on applying the decentralized PKI in the medical health system. Compared with these schemes, we hope to design a more secure, efficient, and suitable Decentralized Blockchain Based-PKI. The following sections outline the proposed scheme based on these goals.

2. METHODOLOGY

2.1. Technologies Uses

2.1.1. Public Key Infrastructure

Internet PKI is an infrastructure in which a CA validates the relationship between an entity and a public key by issuing a public key certificate that contains the distinguished names (DNs) of the entity. This certificate is mainly utilized to verify the identity of a server via HTTPS.

The trust relationships established by a CA are shown in Fig. 1. If the CA receives a certificate signing request, it confirms the identity of the trustee and creates a corresponding certificate. The CA guarantees the identity by signing the certificate with a CA private key. So that the trustor may validate the identity of the trustee, the trustor obtains the certificate and verifies its issuer. If the issuer is confirmed to be a trusted CA by the trustor and the trustee has a private key for that certificate, the trustor trusts the identity of the trustee.

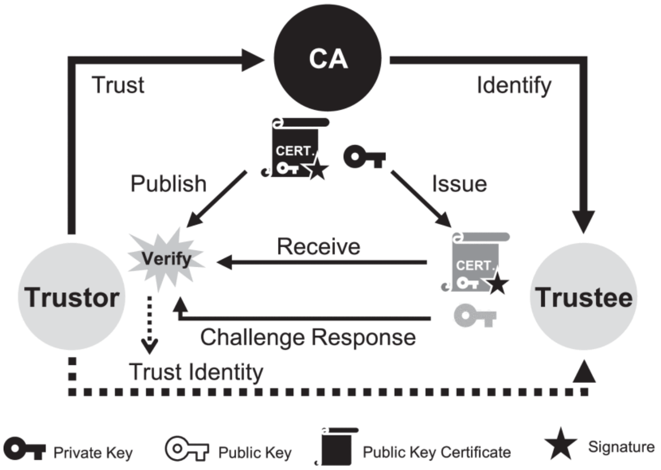

Fig. 1. Trust relationships established by a CA

2.1.2. Hyperledger Fabric

Hyperledger Fabric [8] is a platform for a distributed ledger framework. The ledger conducts data operations in a key-value format without a specific administrator and is managed by multiple peers; the peers have ledgers with the same content and form a distributed ledger network. Data are written to the ledger after an agreement that cannot be changed later is reached among all peers. The data written to the ledger are managed by a set of units called a block. The block has a chain structure with a hash value computed from the previous block using a cryptographic hash function. For this reason, block tampering is detected as a disruption in the chain structure due to the mismatch of the subsequent hash value.

Fig. 2 shows the Hyperledger Fabric scheme. All peers in the distributed ledger network are connected to each other. Each peer has a distributed ledger with the same content and multiple chaincodes (CC), which are also known as smart contracts. The distributed ledger consists of a blockchain and a world state. The blockchain has a journal of transactions that records read/write values (RW-set) to the ledger with a key, and the world state is a key–value store with all values versioned for each transaction.

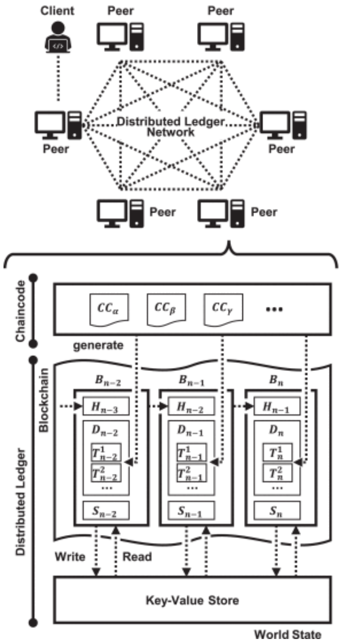

Fig. 2. Description of Hyperledger Fabric [4]

The blockchain consists of multiple blocks arranged in a particular order. Block Bn contains the hash value Hn−1 of the previous block Bn−1 as well as that of block-data Dn and signature Sn created by a block generator. Data Dn includes the transactions Tn={T1n, T2n,…} that connect the RW-set to the world-state. A read/write value in any given transaction cannot be arbitrarily determined.

3. RESULTS AND DISCUSSION

In this study, it is implemented on machine running an Ubuntu 22.04 operating system (Release 2020) using the Docker platform (2021) [9].

This system uses the sample implementation of Hyperledger Fabric (fabric-sample, 2020) [10], which includes the "fabric orderer," and "fabric peer" containers. The roles of these containers are as follows. "Fabric orderer" performs an ordering service, and "fabric peer" performs a peer service. The CAs were implemented using fabric peer containers.

The chaincode was implemented using the Go programming language. It was implemented as a single executable file, and its transactions are selected by arguments. Because data are stored in the ledger in a hierarchical format, this system uses the JSON format (Fig. 3).

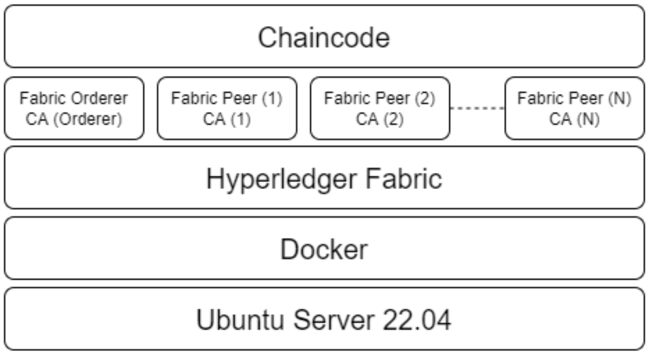

Fig. 3. Decentralized Blockchain-Based PKI System Architecture

3.1. Blockchain Structure

A block is composed of a header and a body, where a header contains hash of the current block, hash of the previous block, timestamp, block number, while block data contains a list of transactions arranged in order, it is written when the block is created by the ordering service.

The Certificates X.509 are stored in the block data with the record of the user's data information such as name, address, phone number, gender and etc. All the data information are protected and secured by hashing mechanism. During the endorsement process, each block data has a record of agreements signed by the endorsers. The items that will be included in the blockchain are shown in Fig. 4.

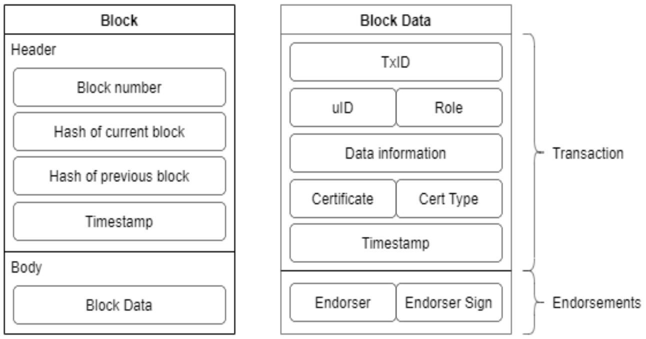

Fig. 4. Contents of a block

3.2. Functionalities

The Hyperledger Fabric SDK (2022) provides the APIs for developing client applications, that can be developed to interact with the blockchain network on behalf of the users. In this case we use hyperledger fabric version 1.4 because version 2.x+ are no longer aims to support the fabric client which provides administrative and management capabilities as shown as in the list of features below:

a. Create Channel

Calls the orderer to start building the new channel. A channel typically has more than one participating organization. To create a new channel, one of the participating organizations should call this method to submit the creation request to the orderer service. Once the channel is successfully created by the orderer, the next step is to have each organization's peer nodes join the channel, by sending the channel configuration to each of the peer nodes.

b. Join Channel

In order for peers to receive blocks from a channel and to invoke chaincode on a channel, it must send a join channel proposal and call the "join channel API" on each peer.

c. Install and Instantiate Chaincode

A chaincode must be installed to peers and instantiated on a channel before it can be called to process transactions. Chaincode installation is simply uploading the chaincode source and dependencies to the peers. This operation is performed on a peer-by-peer basis. Only the peer organization's admin identities are allowed to perform this operation. Instantiating a chaincode compiles, builds, and initializes the chaincode on the peers where the chaincode is installed. When instantiation is complete, the peers can accept chaincode invocations and endorse transactions.

3.3. Chaincode

a. Enrollment process

A patient during registering with the hospital generates a private-public key pair (sk, pk) and signed certificate (cert) by the hospital its own private key. Then, the hospital initiates the enrollment procedure by sending an enrollment request to another unit u_j which is in the consensus group. Then, any unit u_j in the consensus group verifies the claimed certificate and checks if the patient is allowed to join the network by performing the verification procedure (b). Then, u_j signs the proposal and proceeds with the PBFT consensus mechanism with the other units in the consensus group. The block proposal will be added to the ledger only after a successful consensus. Fig. 5 will demonstrate the process of validating the identity of a patient.

b. Verification process

Any unit u_j in the consensus group that has received an enrollment request; verifies if the certificate from the hospital is valid, then u_j signs the received certificate broadcasts to the other units in the consensus group, and proceeds according to steps in the PBFT consensus mechanism.

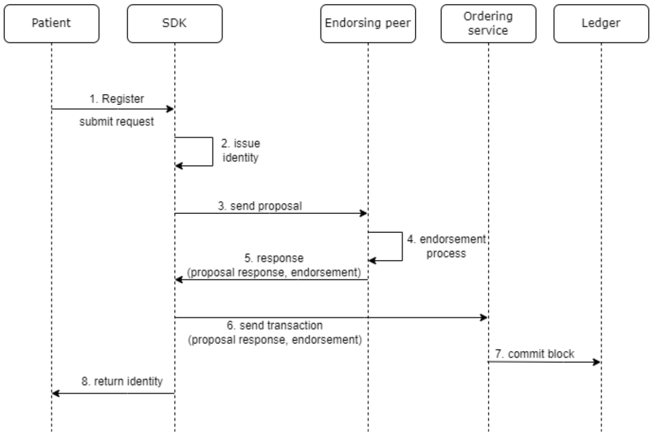

Fig. 5. The process of enrollment the identity of a patient

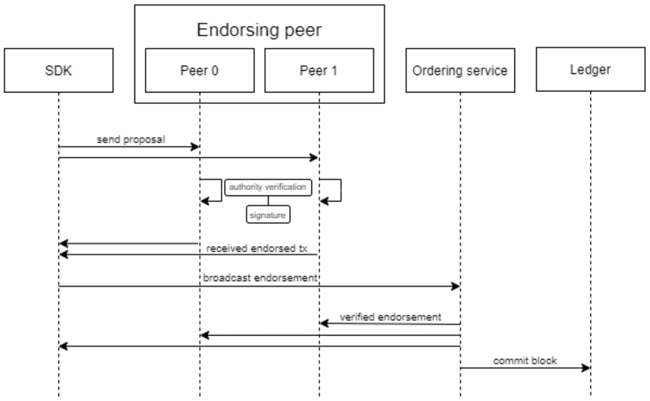

Fig. 6. The process of verifying the identity of a patient

c. Validation process

It is essentially a proof of membership algorithm and is used to verify whether or not a given identity belongs to a given identifier. It naturally considers the revocation status and will respond with true if and only if the certificate is valid and belongs to the given identifier. This can decrease computational costs, especially for resource-constrained environments. Fig. 6 will demonstrate the process of validating the identity of a patient.

d. Revocation process

Any entity unit u_i which is part of the network can initiate the revocation procedure. The revocation procedure starts when u_i finds a reason to revoke an existing certificate of entity u_k in the ledger. This can happen due to bad or malicious behavior, due to the certificate being obsolete, upon request from the owner of a certificate when its private key has been compromised, or other reasons. Entity u_j sends a revocation request and broadcasts it to the consensus group. Any node u_j in the consensus group that has received the revocation request, checks the received proposal and verifies the signature. If both are verified, then, u_j signs the proposal and proceeds with the PBFT consensus mechanism with the other units in the consensus group.

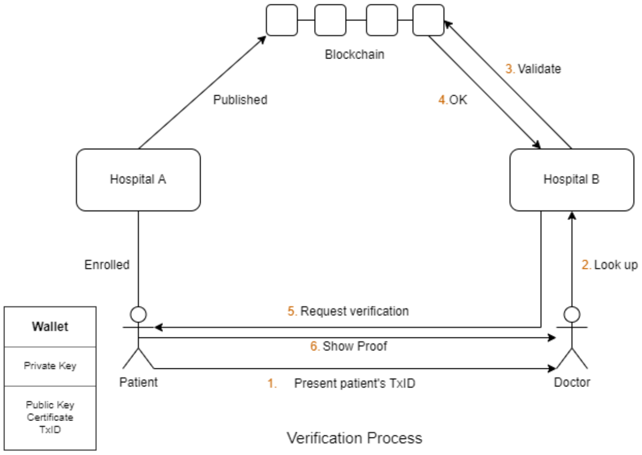

Fig. 7. The process of validation the identity of a patient

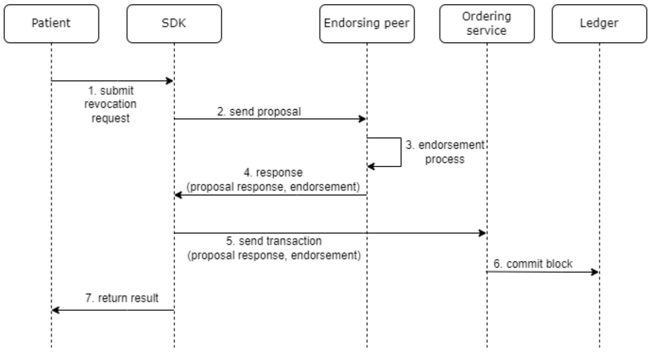
Patient
SDK
Endorsing peer
Ordering service
Ledger
1. submit revocation request
2. send proposal
3. endorsement process
4. response (proposal response, endorsement)
5. send transaction (proposal response, endorsement)
6. commit block
7. return result

Fig. 8. The process of revocation the identity of a patient

e. Update process

The update procedure should naturally include revoking the old certificate by executing Revoke(uID, cert$_{old}$) and registering the new certificate by executing Enroll(uID, cert$_{\mathrm{new}}$) Since Enroll and Revoke procedures require consensus between N numbers of nodes (numbers of pre-selected participant node), for the sake of efficiency, both procedures will be merged, i.e. the block proposal in the consensus mechanism includes records for revoking cert$_{old}$ and enrollment of cert$_{\mathrm{new}}$.

3. CONCLUSIONS

With the growth in scale of decentralized systems, data integrity, security and privacy have become a major concern across the globe and still have limitations in terms of technology. Nowadays, researchers seem to have interested in decentralized blockchain technology, and under their research, it is step-by-step toward perfection and maturity. Hence, this study has proposed a Decentralized Blockchain-based PKI for Patient Identification in the Blockchain Network, using the Hyperledger Fabric, consortium type, which can support organizations having communication on the secure consortium channel, and adopt the Public Key Infrastructure (PKI) to ensure the identity of the data owner while verifying data sources and also establishing trust relationships between entities and verifying communication by digital signatures.

As the result, the decentralized identification model that supports the healthcare domain has been proposed in a developing country Cambodia. This proposed system can apply to various sectors such as healthcare sector it can help establish trust relationships between hospitals, can exchange information between hospitals without concern about the laws or any restrictions, and also helps patients reduce the time and cost expense of having multiple health checks.

ACKNOWLEDGEMENTS

This research is fully funded by the Research Fund Institute of Technology of Cambodia. Moreover, ERASMUS+ Program provides a full-fund research internship at the InfoSec lab of the University of Namur for 3 months.

REFERENCES

[1] TzuMelange, S. (2017, 4 12). History of Risks & Threat Events to CAs and PKI. Retrieved from CAcert Wiki: http://wiki.cacert.org/Risk/History

[2] McKinsey Global Institute. (2019, April 17). Digital Identification: A key to inclusive growth. Retrieved 2022, from https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth

[3] Poston, H. (2021, 9 3). Security of the PKI ecosystem. Retrieved from Infosec: https://resources.infosecinstitute.com/topic/security-of-the-pki-ecosystem/

[4] Kakei, S., Y. Shiraishi, M. Mohri, T. Nakamura, M. Hashimotto and S. Saito. (2020). Cross-Certification Towards Distributed Authentication Infrastructure: A Case of Hyperledger Fabric. IEEE, 8, pp. 135742-135757. doi:10.1109/ACCESS.2020.3011137

[5] Madala, D. S. V., M. P. Jhanwar and A. Chattopadhyay. (2018). Certificate Transparency Using Blockchain. IEEE

International Conference on Data Mining Workshops (ICDMW), (pp. 71-80). doi:10.1109/ICDMW.2018.00018

[6] Yakubov, A., W. M. Shbair, A. Wallbom, D. Sanda and R. State. (2018). A blockchain-based PKI management framework. NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium, (pp. 1-6). doi:10.1109/NOMS.2018.8406325

[7] Bo Qin, Jikun Huang, Qin Wang, Xizhao Luo, Bin Liang, and Wenchang Shi. (2020). Cecoin: A Decentralized PKI Mitigating MitM Attacks. Future Gener. Comput. Syst., 107, pp. 805–815. doi:10.1016/j.future.2017.08.025

[8] Hyperledger Fabric. (2020). A Blockchain Platform for the Enterprise. Retrieved from https://hyperledger-fabric.readthedocs.io/en/release-2.2/

[9] The Docker platform. (2021). Retrieved from https://docs.docker.com/get-started/overview/

[10] Hyperledger Fabric Samples. (2020, Jan). Retrieved from https://github.com/hyperledger/fabric-samples.