J. Math. Math. Sci. (2023) 67–85

A blockchain-based Certificate Management System using the Hyperledger Fabric Platform

Quang Duy Tran (Hanoi, Vietnam)
Trong Minh Hoang (Hanoi, Vietnam)

(Received Nov. 26, 2022)

Abstract. In recent years, blockchain technology, with its outstanding advantages in terms of security and decentralized data storage, has quickly been applied in education, especially in managing educational certificates. The traditional paper certificate management process has many limitations on security, storage, verification, ownership, and prevention of certificate fraud and tampering. With emerging blockchain technology, the traditional paper certificate management process has changed to a new stage with massive benefits and opportunities to overcome the above challenges. Following this approach, many blockchain-based applications have been proposed, and several universities worldwide have adopted various solutions based on blockchain technology. This paper presents implementing an educational certificate management system based on blockchain technology using the Hyperledger Fabric platform. Our proposed solution can be solved in almost storage and security aspects of certificate management problems, such as confidence, verification, ownership, and tamper avoid.

1. Introduction

Blockchain technology is the core technology used to create a cryptocurrency. In 2008, this technology was introduced by Satoshi Nakamoto along with Bitcoin - a cryptocurrency [1]. It has been considered part of the fourth

Key words and phrases: Blockchain, Hyperledger Fabric, Educational Certificate, Verification, Permissioned Blockchain.
2020 Mathematics Subject Classification: 68P25

industrial revolution and was quickly researched and applied in many fields such as finance, insurance, healthcare, the Internet of Things (IoT), supply chain management, intellectual property management, etc.

The development of blockchain technology could be divided into three main stages: Blockchain 1.0, 2.0, and 3.0. Blockchain 1.0 was used for cryptocurrencies. Blockchain 2.0 was introduced along with smart contracts for managing digital properties. A typical case is the Ethereum platform proposed by Vitalik Buterin [6]. In Blockchain 3.0, many applications were developed in various sectors such as government, education, finance, insurance, healthcare, and science [10].

The application of Blockchain to education is still in the early stages. Educational institutions and universities have started to study and utilize blockchain technology. Most institutions use it to secure, share, and verify academic achievement. However, this technology can be applied in many cases, such as issuing the Certificate, storing a portfolio, managing intellectual property, identification, etc. [2]. Many researchers in the field believe that blockchain technology has much more to offer and can revolutionize the field. In the case of certificate management, digital certificates will be stored and secured on a blockchain system. Then, they cannot tamper, and the accuracy of the Certificate can be easily verified by anyone who can access the blockchain system through an application without any third party. Because no intermediary is required to verify the Certificate, the Certificate can still be validated even if the organization that issued it no longer exists. The records of certificates on a blockchain can only be destroyed if all copies stored on network nodes are eliminated.

In this paper, we briefly introduce applications of blockchain technology in the education field, educational certificates, and certificate management process and exploit the advantages of certificate management based on blockchain technology. We also propose a digital academic certificate management solution based on the Hyperledger Fabric platform. The rest of the article is structured as follows. Section 2 presents mainly related work. In section 3, we illustrate a brief overview of blockchain technology. Section 4 outlines the certificate management process and the types of different certificates. In Section 5, we propose an educational certificate management solution. Last but not least, we conclude this article in Section 6.

2. Related Works

With its outstanding features, blockchain technology could benefit the education field significantly. Recently, numerous blockchain-based apps for educational purposes have been developed, and extensive studies and analyses on Blockchain in the field of education have been conducted. Blockchain-based applications were classified into 12 main categories, including certificates management, competencies, and learning outcomes management, evaluating students' professional ability, protecting learning objects, securing collaborative learning environment, fees and credits transfer, obtaining digital guardianship consent, competitions management, copyrights management, enhancing students' interactions in e-learning, examination review, and supporting lifelong learning. Each category addresses security, identity authentication, trust, and privacy issues within the education environment [15].

In the case of certificate management, it concerns handling all forms of academic certificates, transcripts, or other accomplishment records. Many applications that used blockchain technology for managing digital certificates were proposed. And many educational institutions and universities worldwide have applied this technology to manage and issue their digital education certificates. In 2017, The University of Nicosia (UNIC) issued and validated certificates using a public blockchain based on the open-source standard "Blockcerts". The Knowledge Media Institute (KMI) within Open University(OU), United Kingdom (UK), has performed a study on enhancing standards for badging, certification, and reputation on the Web with the use of blockchain technology. In addition, the Massachusetts Institute of Technology (MIT) has used the Learning Machine (LM) Certificates to issue digital diplomas for students at the MIT Media Lab [2]. Sony Global Education has also developed an internal certification management system and a system that applies to the education sector using blockchain technology [3].

Some innovative digital educational certification platforms using blockchain technology were also proposed. Nespor [16] proposed a blockchain-based certification platform that compensated for using the school as a certification agent. This platform would authorize universities or educational institutions to supply official certificates for students with a high level of privacy of their information. Thus, students could share it directly with anyone requesting their certificates. Authors in [17] introduced a novel blockchain-based education solution for issuing and verifying official transcripts or certificates. The individuals could have access to their data records and can easily share those records with others. However, only certified organizations can access and modify the stored data

under some restricted conditions and rules. Srivastava et al. [18] proposed a globally trusted blockchain-based educational framework among various stakeholders like universities, companies, and other educational institutions that agree to collaborate as a part of the framework. This framework supports verifying the academic certificates and course credits of a learner registered in a university or an educational institution which can be digitally transferred among the stakeholders. All stakeholders know students' education records by achieving consistency among the local copies of educational certificates and credits.

3. Blockchain Technology Background

Blockchain technology combines cryptographic theory, game theory, and techniques in computer science. This section outlines the key concepts and components used in this technology.

Blockchain. Blockchain is a block sequence containing a complete list of cryptographically signed transaction records, called a digital ledger [1]. Each block is cryptographically linked to the previous block after the validation process. When new blocks are created, they are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using previously established rules. The first blockchain block is called the genesis block, which has no parent block. A typical blockchain is shown in Figure 1.

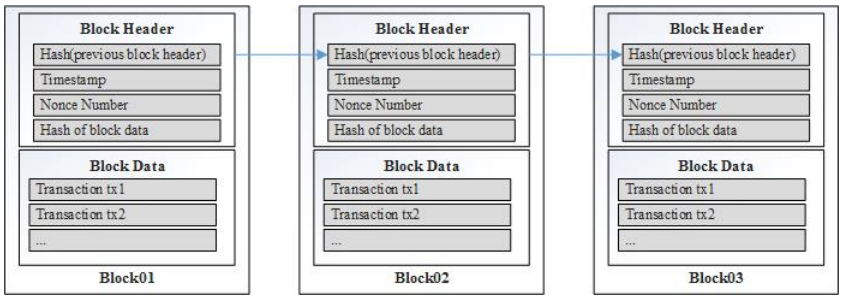

Figure 1. A typical Blockchain

Block. A block contains a block header and data (as shown in Figure 1). The block header contains metadata for this block. The block data includes a list of validated transactions published to the blockchain network. It should be noted that they can define their data fields in the different blockchain systems.

However, many blockchain systems have data fields like the following:
The block header includes data fields as

- Previous block header's Hash: a hash value that points to the previous block.
- Hash of block data: the hash value of all the transactions in the block
- Timestamp
- Nonce Number: used for every hash calculation

The block data is composed of a transaction list. The maximum number of transactions a block can contain depends on the block size and the size of each transaction.

Cryptographic Hash Functions. These functions are used for many operations in the Blockchain. Hashing applies a cryptographic hash function to input data, which calculates a relatively unique output (called a digest or a hash code). Input data can be nearly any type (e.g., a file, text, or image). Anyone can take input data, hash that data, and derive the same result. This proves that there was no change in the data. Even the smallest change to the input data (e.g., changing a single bit) will result in a completely different output digest [4]. Within a blockchain network, hash functions are used for many tasks, such as: creating unique identifiers, combining with the public key to derive addresses, and securing the block data and header.

Asymmetric-Key Cryptography. Blockchain uses asymmetric-key cryptography (public-key cryptography) [5]. Asymmetric-key cryptography uses a pair of keys: a public key and a private key. These keys are mathematically related to each other. The public key is made public, but the private key must be kept secret. Although there is a mathematical relationship between the two keys, the private key cannot be determined based on knowledge of the public key. Data can be encrypted with the public key and then decrypted with the private key.
Asymmetric-key cryptography enables a trusting relationship between users who do not know or trust one another by verifying the integrity and authenticity of transactions. A private key is used to encrypt transactions to create a digital signature of the transaction to do. The digital signature of the transaction is broadcasted throughout the whole network, and anyone also can use public keys to verify the digital signatures. Since the public key is always public, encrypting the transaction with the private key proves that the signer of the transaction has access to the private key. Alternatively, one can encrypt data with a user's public key such that only users with access to the private key can decrypt it.

In Blockchain, private keys create a digital signature by encrypting the transaction. Public keys verify digital signatures generated with private keys and derive addresses.

Consensus mechanism. Most blockchain systems use consensus protocols to reach consensus among untrustworthy nodes in decentralized environments. In the existing systems, there are many consensus mechanisms, such as Proof-of-Work (PoW) [1], Proof-of-Stake (PoS) [6], Practical Byzantine Fault Tolerance (PBFT) [7], and RAFT [8], etc.
PoW is a consensus protocol used in the Bitcoin network [1]. In a decentralized network, a node wants to publish a block of transactions and add this block to the Bitcoin blockchain to get rewards, and much work has to be done to prove that the node is not likely to attack the network. The nodes repeatedly run hashing functions to find a Nonce value, which is challenging but easy for others to validate. This enables all other nodes to validate any new blocks quickly, and any proposed block that is not satisfied will be rejected.
Proof-of-Stake (PoS) is used in Ethereum [6]. The PoS model is based on the idea that the more stake a user has invested into the system, the more likely they will want the system to succeed and the less likely they will want to subvert it. The stake is often an amount of coin the blockchain network user has invested into the system in various ways. PoS blockchain networks use the amount of stake as a determining factor for publishing new blocks. Thus, the capability of a blockchain network user to publish a new block is dependent on the ratio of their stake to the overall blockchain network amount of staked coin. There is no need to perform resource-intensive computations as found in POW with this consensus model. So, Compared to PoW, it saves more energy and is more effective.
Practical Byzantine Fault Tolerance (PBFT) [7] and RAFT [8] [9] are consensus protocols used in different versions of the Hyperledger Fabric platform. They are used in the ordering service, which receives endorsed transactions from the clients and emits a stream of blocks.

4. Certificate considerations

In this session, the main characteristics of a certificate and its management system will be presented to figure out how to apply blockchain technology to this area.

4.1. Certificate Concept

A certificate contains a certified statement, especially about the truth of something. In education, the Certificate is used as evidence for the achievement of learning outcomes, the teacher's competence, a learner's learning process, etc. Certification describes any process by which a certificate is issued to verify a claim [2].

4.2. Processes involved in the certification

There are three processes involved in certification including:

Issuing. This is the process of generating and recording certificate data such as certificated requests, certificate issuer, evidence, recipient, and signature onto a certificate. Usually, this data is stored in a centralized database and on a certificate issued to the user.

Sharing. The recipients will share their certificates with a third party in this process. There are three methods to sharing credentials: directly transferring the Certificate (or a copy of the Certificate) to the third party; storing the Certificate with an authorizer who is only allowed to share with specific people according to your request; publishing the Certificate by putting it in an online public store, where everyone may view it.

Verification. In this process, a third party will verify the Certificate's authenticity. There are three ways to do this

- Verification uses security features built into the Certificate, such as checking the seal's authenticity, special security paper, signature, etc.
- Verification of Certificate through the original issuer whereby a third party contacts the original issuer to ask whether they issued the Certificate.
- Verification utilizing an application that can access a centralized database provided by the issuer. Anyone can look up certificates in this database to see copies of all issued certificates. Level and compare the two versions with each other.

4.3. Limitations of Paper Certificates

Most certificates and records are still issued on paper and are widely used. However, paper certificates also have the following significant disadvantages [2]:

- Paper certificates are easy to forget. Therefore, the issuer must store a list of the issued certificates for verification. This verification is a manual process; hence, it is time-consuming and requires considerable human resources.

- While certificates may still be valid, the ability to verify them is lost if the issuer no longer exists.

- The more secure the Certificate, the Certificate cost is the more expensive.

- Issuers can cheat when issuing certificates without any restrictions.

- Once a certificate has been issued, there is no way to revoke the Certificate unless the owner relinquishes control of it.

4.4. Digital Certificates not using Blockchain Technology

Digital certificates are issued without using a blockchain system and have many advantages over paper certificates, such as:

- They use fewer resources to issue, maintain and use because the verification process can be done automatically. The security of a certificate is based on the security of cryptographic protocols, which assures that it is inexpensive to make but prohibitively expensive for anybody other than the issuer to reproduce.

- Issuers can revoke certificates.

- Some issuer fraud is not possible, such as changing the timestamp, changing the Certificate's serial number, etc.

However, this digital Certificate also has some significant disadvantages, such as:

- If not using digital signatures, they are still straightforward to forget.

- If digital signatures are used, the issuance and verification of certificates significantly depend on third parties who are digital signature providers.

- Keeping digital certificates safe can require complex backup systems.

4.5. Digital Certificates using Blockchain Technology

Blockchain technology is considered ideal for securing, sharing, and verifying certificates. Once certificate information is stored on a blockchain system, it cannot be altered or tampered with. As a result, blockchain-secured digital certificates hold significant advantages over paper certificates or other digital certificates (non-blockchain), such as:

- They cannot be tampered with.
- Verification of the Certificate is done easily by anyone through a piece of software without any intermediary parties.
- A certificate can still be validated even if the organization that issued it no longer exists or has an access system.
- Certificates can only be destroyed if every copy of the ledger on every node in the blockchain system is destroyed.
- Using a Hash of the document allows the document's signature to be published without needing to publish the document itself, thus ensuring its privacy.

5. The proposed platform for the education certificate management system

5.1. Scope and requirements

An educational certificate management system is built on a blockchain platform that focuses on solving problems in certificate management, such as security, authentication, and ownership, with specific requirements as follows:

- The issuers who want to participate as a system member must be predefined and licensed.
- The certificates stored on the blockchain system must be secure and cannot be tampered with. These certificates have to be verified easily and quickly by third parties who need to verify the certificates. The input to the solution is the certificate information. Certificate information includes the Certificate number, issuer's information, recipient's information, Certificate's content, expiration date, the status of the Certificate, etc.

- Build an application that helps issuers manage statistics certificates and the life cycle of certificates through the functions such as data input function, search, statistics, etc.

- Providing functions that allow recipients to share certificates and manage their certificates.

- Providing tools to help third parties(such as employers, educational institutions, etc.) verify certificates easily and quickly. Reduce time for validating a certificate.

5.2. Designing system

A. System architecture

We designed the education certificate management system based on the Hyperledger Fabric platform with the given requirements (Figure 2). Permissioned blockchain platforms are increasingly used in industry. To find the most suitable blockchain platform to design and implement an education certificate management system, we review and assess the three leading permissioned blockchain platforms: Hyperledger Fabric, Quorum, and R3 Corda, concerning performance, scalability, privacy, and other criteria.

Hyperledger Fabric is an open-source permissioned blockchain platform developed by the Linux Foundation community. It is designed for enterprise contexts and delivers critical differentiating capabilities over other popular distributed ledger or blockchain platforms [13]. The Fabric uses smart contracts (also called chaincodes) to implement the application logic. In this platform, consensus protocols can be plugged in (such as Practical Byzantine Fault Tolerance (PBFT), Raft or Kafka,...). With a highly modular and configurable architecture, Hyperledger Fabric is one of the permissioned blockchain platforms that can be applied in many fields, such as finance, banking, healthcare, human resources, supply chain, and even digital music delivery, etc. Walmart used Hyperledger Fabric to take on food traceability and safety. Sony Global Education chooses Hyperledger Fabric for its Next-Generation Credentials Platform [14].

R3 Corda is an open-source permissioned platform developed by R3 Corporation Corda's design was initially driven by the needs of regulated financial institutions but turned out to be far more broadly applicable [21]. Corda also uses smart contracts for implementing the application logic. It has two types of consensus: the validity of the transaction and the uniqueness of the transaction. Each signer checks validity before signing the transaction, and the Notary nodes check uniqueness. The consensus is reached by the nodes that carry out the transactions, not the entire system.

Quorum is an enterprise blockchain platform initially developed by J.P. Morgan for the financial sector but can be used for any industry. Quorum is a permissioned blockchain based on the Ethereum blockchain [23]. More precisely, it is a fork from go-Ethereum, with several better modifications regarding privacy, consensus protocol, performance, etc. It uses other consensus protocols for consortium blockchains, such as a Raft-based consensus protocol and Istanbul BFT [20].

Table 1 provides an essential characteristics summary of the three above blockchain frameworks [19] [20] [22].

Characteristics	**Hyperledger Fabric**	**R3 Corda**	**Quorum**
Governance/Support	Linux Foundation	R3 Corporation	J.P. Morgan Chase
Mode of operation	Permissioned	Permissioned	Permissioned
Consensus	Plug-in consensus mechanism	Voting-based/RAFT	Clique PoA of RAFT-based or Istanbul BFT
Smart contracts	Yes	Yes	Yes
Privacy	Channels and private data collections permit high customization	Transactions are private by default. Information shared on a need-to-know basis	Supports private and public transactions
Performance	Strongest latency and throughput values	Strongest latency, poor throughput	Poor latency, strong throughput

Table 1. Comparison of Hyperledger Fabric, R3 Corda, and Quorum.

Three types of users are involved in this proposed system: Recipients, Issuers, and Verifiers. Recipients are students or course participants. Each recipient will be assigned a username and password to access the Web application. Issuers are the educational institutions or universities that issue the Certificate to the recipients. Verifiers are the companies, employers, or educational institutions that need to verify the accuracy of the Certificate. The proposed system includes the following main components:

Blockchain system. Is a permission blockchain network designed based on the Hyperledger fabric platform. Details of this network are described in

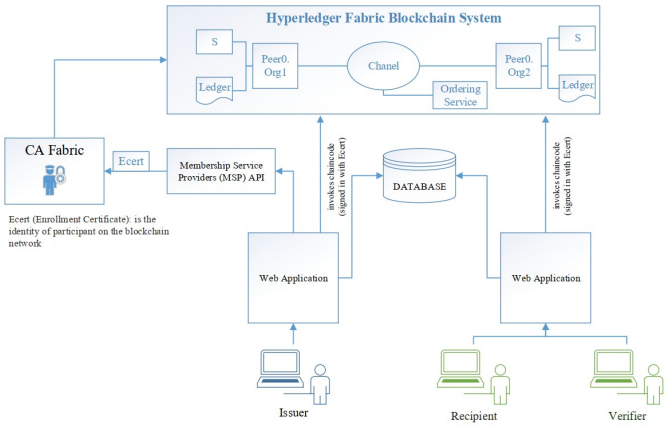

Figure 2. The proposed blockchain-based certificate management system architecture

the next section.

Web application for issuers. The application is built on the web platform. This application can connect to the Peer in the blockchain network and update query ledgers through smart contract calls. It includes the following functions: Register creates a certificate, update certificate information, view the Certificate in detail, search, certificate statistics, etc.

Web application for recipients and verifiers. This application is also built on a web platform and includes the recipient's and verifier's functions. The functions for recipients include sharing certificates, searching, view certificate in detail. The tasks for verifiers include: Looking up, verifying Certificates, etc.

Database. Is a database that stores attribute information, including information about the recipient, educational institution, Certificate, etc., as well as the user's login information.

B. Proposed blockchain model

Figure 3 depicts the hyper ledger fabric-based blockchain system architecture we designed and implemented for the certificate management solution.

The blockchain network consists of Peers (called Peer nodes), Endorsing Peers, the Ordering Service, and Certificate Authorities (CA). Each Peer hosts ledgers and smart contracts (in Hyperledger Fabric are called chain code). The endorsing peers are responsible for endorsing the transaction proposals before sending them to the ordering service. Peers work together through a channel called "EduChanel." The ledger stores the basic information of the Certificate. The Peers update and query certificate information on the ledger through pre-

installed smart contracts. The ordering service includes three nodes. The Raft consensus protocol is used in the ordering service for creating new blocks.

When each organization joins the network, it owns two peers; one Peer is the endorsing Peer and Certificate Authority (CA). A user or a node wants to participate in the blockchain network to have a digital identity issued by a CA. Digital identities (or simply identities) have the form of cryptographically validated digital certificates that comply with the X.509 standard.

In this network, Fabric CA is used for each organization. As shown in Figure 3, organization Org1 will own Peer.O1, Endorsing Peer.O1, and CA1. CA1 issues digital identities for users of the Org1.

The blockchain network has two main operations: updating certificate information and querying certificate information. The update creates a new record of certificate information and updates it to the ledger on the Peers after the verification and consensus process. An information query is an action in which users can retrieve certificate information stored on the ledger at each Peer in the system.

The process of updating certificate information from the application to the ledger is briefly described in the following steps:

- Step 1: Initiates a transaction proposal
  When the user enters the Certificate's information (including the Certificate's attribute information and image) into the system through the web application's functions, the web application generates a transaction proposal. It sends it to the endorsing peers in the blockchain network for endorsement (through API functions provided by Fabric SDK). The proposal is a request to invoke a chain code function with input parameters such as certificate information, sender, etc., to read and update the ledger.

- Step 2: Endorsing a proposal
  Each of these endorsing peers validates the transaction proposal by independently executing a chain code using the transaction proposal to generate a transaction proposal response, signs it, and returns it to the application.

- Step 3: Receiving signed transaction proposal response
  The application receives a signed transaction proposal response from the endorsing peers. The application verifies the endorsing peer signatures and compares the proposal responses to determine if the proposal responses are the same. Then, the application generates a transaction with a transaction proposal and a signed transaction proposal response.

- Step 4: Submitting transaction

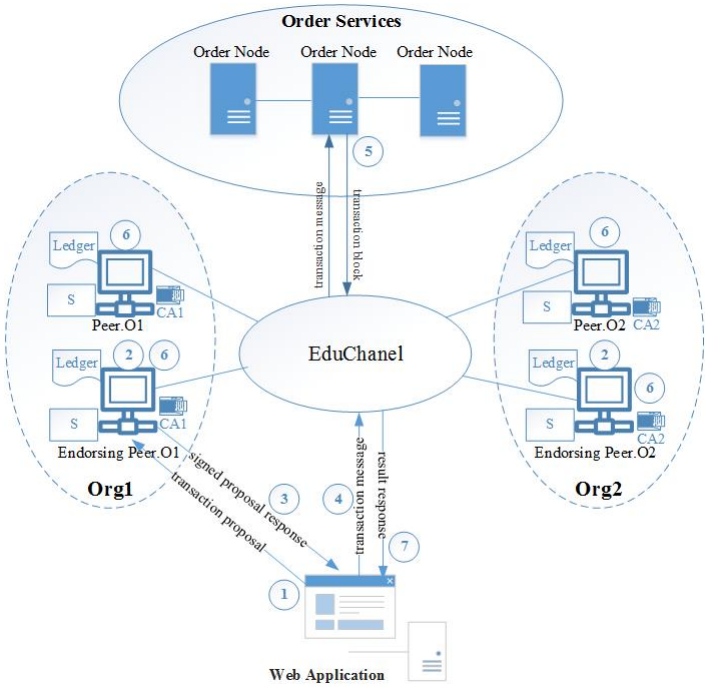

Figure 3. The proposed blockchain network architecture

The application sends the transaction to the ordering service node by "broadcasting" it through the " EduChanel " channel.

- Step 5: Packaging and Delivering blocks
  Since ordering service nodes receive the transaction, the order, and package transactions into a block, the ordering service nodes work together under the RAFT consensus mechanism for the publishing block. This is to ensure that a unique block is generated on the system. When the publishing block of transactions is completed. The block of transactions is distributed to all peers on the channel.

- Step 6: Ledger updated
  The peers receive a block of transactions from the ordering service; every transaction within a block is validated before it is committed to the ledger. Valid transactions are committed to the ledger. Invalid transactions are retained for audit but are not committed to the ledger.

- Step 7: The application receives the transaction result response
  When peers committed the transaction to their local ledger. Each Peer

emits an event of transaction result to notify the application that the transaction was validated or invalidated. The application receives the results of executing the transaction from the peers and displays them to a user.

Querying certificate information is much simpler than updating. The application sends a query proposal to the Peer for invoking the smart contracts. The Peer executes smart contracts to query information from its local ledger and returns the query result to the application.

5.3. Implementation

A. Blockchain System

We implement Hyperledger Fabric based blockchain system in Ubuntu 18.04 operating system. Docker is used for developing, implementing, and running peers, applications, and services. Therein, each Peer, application, or service is installed and running on a distinguished docker container.

The details of the deployment environment are as follows:

- Operating system: Ubuntu 18.04
- Hyperledger fabric version 2.2.2
- Hyperledger fabric CA Client version 1.4.9
- CouchDB Database version 3.1.

We deployed the blockchain system with assuming that there are two organizations in the system: Org1 and Org2. Each organization includes two peers: a normal Peer, an endorsing Peer, and a CA. Each Peer and CA are deployed and run on a distinguished container. In this system, we also use three ordering nodes for ordering service. They are also installed and run on a distinguished container.

Ledger. Ledger at a peer is stored on CouchDB database version 3.1. A few pieces of information are stored in the ledger, including the Name of the Issuer; ID of the Recipient; Hash of certificate data; Signature of the Issuer (The private key of the issuer signs the signature); Signature of the recipient (The private key of recipient signs signature), Certificate's date was created, etc.

Smart Contract. There are a few main smart contracts that are deployed and run in chain code at the Peer as follows:

- CreateNewCertificate: Issues and writes a new certificate to the ledger. The input information includes: Name of the Issuer; ID of the Recipient; Hash of certificate data; Signature of the Issuer (The private key of the issuer signs the signature); Signature of the recipient (the private key of the recipient signs the signature), Certificate's date was created, etc.
- CancelCertificate: revoke the issued Certificate for recipients. The input information includes the ID of the Certificate.
- GetCertificateByIssuer: Returns all the certificates issued by a specific Issuer. The input information includes the Public Key of the Issuer that issued the Certificate.
- GetCertificateByRecipients: Public Key of Recipient
- QueryCertificateByID: Get a detail of the Certificate based on its ID.

B. Web application for issuers

This web application is developed using Javascript language on the NodeJS platform version 12.12.0. This application includes the main functions:

- Sign in: allows issuers to log in to the application.
- Sign out: exit the application.
- Create Certificate: issues a new certificate for recipients. Including information: Name, Date of birth, year of graduation, Degree classification, Date of issue, and Image of Certificate.
- Cancel Certificate: revokes the issued Certificate.
- View certificates: views issued certificates.

C. Web application for recipients and verifiers

This web application is also developed using Javascript language on the NodeJS platform version 12.12.0. The main functions for recipients:

- Register: allows recipients to sign up for receiving Certificates.
- Sign in: allows recipients to log into the application.
- Sharing certificates: allows recipients to share their Certificates.
- View certificate: allows recipients to view their Certificate in detail. The functions of verifiers:

- Verify Certificate: this function allows verification Certificate based on Certificate's image or Certificate Hash that the recipient supplies.

D. Database

This database stores data of Web applications, using MongoDB database system version 5.05; stored information includes:

- Certificate: ID of the certificate, recipient's name, recipient's major, issuer's name, etc
- Recipient: Recipient ID, name, email, password, etc.

6. Conclusion

In this paper, we briefly presented an overview of applying blockchain technology in the education field and its advantages in the management of digital educational certificates. In addition, we have proposed an educational certificate management system based on the Hyperledger Fabric platform. The blockchain network architecture and the process of updating and querying certificate information are also presented in detail. This solution meets the requirements for certificate management, such as security, sharing, ownership, and verification. We have also successfully implemented this solution in a test environment. In the future, we hope to continue this solution in transcripts management and implement it in practice.

References

[1] **Nakamoto.,** *Bitcoin: A peer-to-peer electronic cash system,* Decentralized Business Review, p.21260, (2008)

[2] **Alexander Grech, Anthony F. Camilleri, Andreia Inamorato dos Santos,** *Blockchain in Education,* European Commission JRC, 2017.

[3] **J. Russell,** *Sony wants to digitize education records using the Blockchain,* https://techcrunch.com/2017/08/09/sony-education-blockchain, last accessed 2022/11/12.

[4] **National Institute of Standards and Technology,** *Secure Hash Standard (SHS).* Federal Information Processing Standards (FIPS) Publication 180-4, August 2015, https://doi.org/10.6028/NIST.FIPS.180-4.

[5] **D. Johnson, A. Menezes, and S. Vanstone,** *The elliptic curve digital signature algorithm (ecdsa),* International Journal of Information Security 1(1), 36-63 (2001).

[6] **Vitalik Buterin,** *A Next-Generation smart contract and decentralized application platform*. Ethereum White Paper.

[7] **Christian Cachin**: Architecture of the Hyperledger blockchain fabric. IBM Research (2016).

[8] **Diego Ongaro and John Ousterhout,** *In Search of an Understandable Consensus Algorithm (Extended Version),* https://raft.github.io, last accessed 2022/04/12.

[9] **Artem Barger, Yacov Manevich, Hagar Meir, Yoav Tock,** *A Byzantine Fault-Tolerant Consensus Library for Hyperledger Fabric,* arXiv:2107.06922 [cs.DC], 2021.

[10] **Gatteschi V, Lamberti F, Demartini C, Pranteda C, Santamaría V.,** *Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?,* Future Internet. 2018; 10(2):20. https://doi.org/10.3390/fi10020020

[11] **P. K. Sharma, M.-Y. Chen, and J. H. Park,** A software-defined fog node based distributed blockchain cloud architecture for IoT. IEEE Access, PP(99):1-1 (2017).

[12] **Protocol-Labs,** *Filecoin: A decentralized storage network,* https://filecoin.io/filecoin.pdf, last accessed 2022/11/22.

[13] **Hyperledger,** *Fabric,* https://www.hyperledger.org/, last accessed 2022/11/22

[14] **Hyperledger.Org,** *Browse various use cases powered by Hyperledger technologies,* https://www.hyperledger.org/learn/case-studies, last accessed 2022/11/22

[15] **Alammary A, Alhazmi S, Almasri M, Gillani S.,** *Blockchain-Based Applications in Education: A Systematic Review,* Applied Sciences. 2019; 9(12):2400. https://doi.org/10.3390/app9122400.

[16] **Nespor, J.,** *Cyber schooling and the accumulation of school time,* Pedag. Cult. Soc. 2018, 1–17. https://doi.org/10.1080/14681366.2018.1489888

[17] **Han, M.; Li, Z.; He, J.S.; Wu, D.; Xie, Y.; Baba, A.,** *A Novel Blockchain-based Education Records Verification Solution,* In Proceedings of the 19th Annual SIG Conference on Information Technology Education, Fort Lauderdale, FL, USA, 3–6 October 2018; pp. 178–183. https://doi.org/10.1145/3241815.3241870

[18] **Srivastava, A.; Bhattacharya, P.; Singh, A.; Mathur, A.; Prakash, O.; Pradhan, R.,** *A Distributed Credit Transfer Educational Framework based on Blockchain,* In Proceedings of the 2018 Second International Conference on Advances in Computing, Control and Communi-

cation Technology (IAC3T), Allahabad, India, 21–23 September 2018; pp. 54–59. https://doi.org/10.1109/IAC3T.2018.8674023

[19] **Valenta, Martin; Philipp G. Sandner,** *Comparison of Ethereum, Hyperledger Fabric and Corda,* 2017, http://explore-ip.com/2017_Comparison-of-Ethereum-Hyperledger-Corda.pdf, last accessed 2023/01/23.

[20] **20. Julien Polge; Jérémy Robert; Yves Le Traon,** *Permissioned blockchain frameworks in the industry: A comparison,* ICT Express, Volume 7, Issue 2, 2021, pp. 229-233,ISSN 2405-9595. https://doi.org/10.1016/j.icte.2020.09.002.

[21] **Richard Gendal Brown,** *The Corda Platform: An Introduction,* 2018, https://corda.net/content/corda-platform-whitepaper.pdf, last accessed 2023/01/23.

[22] **Fausto Martin,** *Permissioned Blockchain Platform Comparison,* https://www.tradeheader.com/blog/hyperledger-fabric-comparative, last accessed 2023/01/23.

[23] **Quorum,** *Quorum WhitePaper,* https://www.blocksg.com/single-post/2017/12/27/quorum-whitepaper, last accessed 2023/01/23.

Tran Quang Duy
Information Technology Faculty, Thang Long University
Hanoi
Vietnam
duytq@thanglong.edu.vn

Hoang Trong Minh
Telecommunication Faculty, Posts and Telecoms Institute of Technology
Hanoi
Vietnam
hoangtrongminh@ptit.edu.vn