International Journal of Software Engineering and Its Applications
Vol.13, No.2 (2019), pp.1-8
http://dx.doi.org/10.21742/ijseia.2019.13.2.01

Design and Implementation of a Personal Portfolio Multilateral Authentication System Based on Hyperledger Fabric

Junho Jeong[1], Donghyo Kim[2], Yangsun Lee[3*], and Yunsik Son[4*]

[1]Dept. of Computer Science and Engineering, Kongju National University, Cheonan, Korea
[2]Dept. of Computer Science and Engineering, Dongguk University, Seoul, KOREA
[3]Dept. of Computer Engineering, Seokyeong University, Seoul, Korea
[2]yslee@skuniv.ac.kr, [3]sonbug@dongguk.edu

Abstract

Although the blockchain technology has been developed mainly around bitcoin, it is also being studied for use in various fields. As a result, it is spreading not only to the applications of settlement and transaction utilizing the characteristics of bitcoin (virtual money) but also to the fields not directly related to money. In this paper, we propose a personal portfolio multi-lateral authentication system that guarantees the reliability and integrity of data by using the features of blockchain technology on a distributed network. The proposed system could be submitted learning data to a peer in a distributed network by a learner. Then, it is verified through an agreement between peers and recorded in a chronologically encrypted ledger. It is a system that provides learners' information in a safe and prompt manner between schools, the school to the certification authority, the school to the company, and the student to the company according to decisions of learners.

Keywords: *Multilateral authentication, Blockchain, Hyperledger fabric, Chaincode, portfolio management, Blockchain performance measurement*

1. Introduction

1.1. Necessity of study

The Blockchain, known worldwide as the core technology of the cryptocurrency Bitcoin, is currently examining the feasibility and promoting the introduction of technology in most industries including finance, manufacturing, distribution, public and medical [1][2]. The reason why the blockchain is used in various industries is the technical characteristics of the blockchain, the biggest characteristic of which is based on the distributed ledger technology that shares and manages the transaction data by agreement in a distributed system environment. This provides a difficult environment for deleting or manipulating data. This systemic characteristic enables a business network environment that enables transparent transaction processing based on trust [3][4].

In Korea, all education-related evaluation agencies such as schools, companies, institutions, etc. now utilize a centralized system that directly manages learner's data, which connects and integrates distributed data and information systems to provide. However, the system is that all

Article history:
Received (March 26, 2019), Review Result (June 17, 2019), Accepted (August 28, 2019)

Print ISSN: 1738-9984, eISSN: 2208-9802 IJSEIA

servers are integrated at the city and provincial office of education. So, if the central server is attacked, it is possible to leak the organization's operational matters and sensitive personal information of students. In addition, according to a recently reported article, there has been a case of manipulating the life record book by collaborating between teachers and students [5].

In order to solve this problem, this paper proposes a system for managing learner's learning information by using distributed ledger with reliability and transparency.

2. Related researches

2.1 Educational administration information system in KOREA

The NEIS, a national educational administration information system used in Korea, is a system that electronically processes all educational administrative information. All elementary, middle, high, and special schools nationwide, 182 regional school boards, 16 cities, provincial offices of education, and the Ministry of Education and Science are connected by the Internet [5]. The database server is installed in the national provincial offices of education, and the provincial offices of education maintain administrative support. It is organized to manage matters, school life and grades.

However, since NEIS has a database server integrated with the metropolitan and provincial offices of education, institutional information can be leaked if the central server is attacked. And, although the teacher has logged in with the authority of the commercial classroom curriculum, there is a problem in that the grade file of another subject is accessible. In addition, there is a problem that the reliability and transparency of NEIS is always raised because there is a problem that when the grade file is modified, only the record of the last modifier is left without the login record of the previous modifier.

2.2 Distributed ledger and blockchain

A distributed ledger is a consensus technique for digital data that is replicated, shared, or synchronized [6]. The data in distributed ledgers may be geographically distributed across sites, countries or agencies. This distributed data is synchronized when all requests are written by the user, sharing the state with all systems, allowing each system to store the state. At this time, the synchronization method follows a consensus rule existing between each system, and once agreed, the content is applied to all systems. Therefore, in the distributed ledger system, all participating individual systems have their own ledger data and always synchronize, and one of the methods of state sharing and consensus formation for this is blockchain technology.

Blockchain is a digital ledger where information about transactions in a distributed network is shared among network participants [7]. In other words, blockchain is a data structure for implementing distributed ledger, and all transaction blocks that have been agreed and validated by network participants are connected to the most recent block from the beginning of the chain. Therefore, the participating member can check only the transactions of the participants of the same channel as their own. In order to manage transactions in the system of the existing server/client environment, authentication is performed by using a third party. In contrast, in the blockchain network, the contents of the ledger are agreed. In addition, verification using digital signature using hash algorithm is performed to ensure transaction integrity. Due to the nature of the blockchain, there are three major categories: public blockchain, private blockchain, and consortium blockchain.

Hyperledger Fabric [8] is an open-source framework for building blockchain network infrastructure for Business-to-Business (B2B) and Business-to-Consumer (B2C) transactions.

Hyperledger Fabrics is also different from the public blockchain that anyone can participate in. Only users registered with the Membership Service Provider (MSP) and channel can participate in the blockchain network in Hyperledger Fabric.

[Figure 1] is a model architecture of the Hyperledger Fabric. Not only can all users own the ledger and share all the information on the network equally, but in the case of sensitive information, it shows how the channel is organized only between separate participants.

Hyperledger Fabric consists of a blockchain network, certificate authority server, and client. Generally, membership information such as Peer's authority and orderer's authority defined in client is registered on the server and encryption of digital certificate, public key, private key, etc. The data, first block, genesis block, and transaction generator are created and distributed to the Hyperledger Fabric network. Then, based on the distributed encryption data, the Hyperledger Fabric network always maintains peers and orderers. When transactions are executed by smart contracts, peers verify the results and check the various digital certificates. They collect and sort verified transactions and generate blocks. This separation of tasks can reduce the load on peers executing and verifying transactions, and parallel processing of two or more tasks simultaneously can improve system performance.

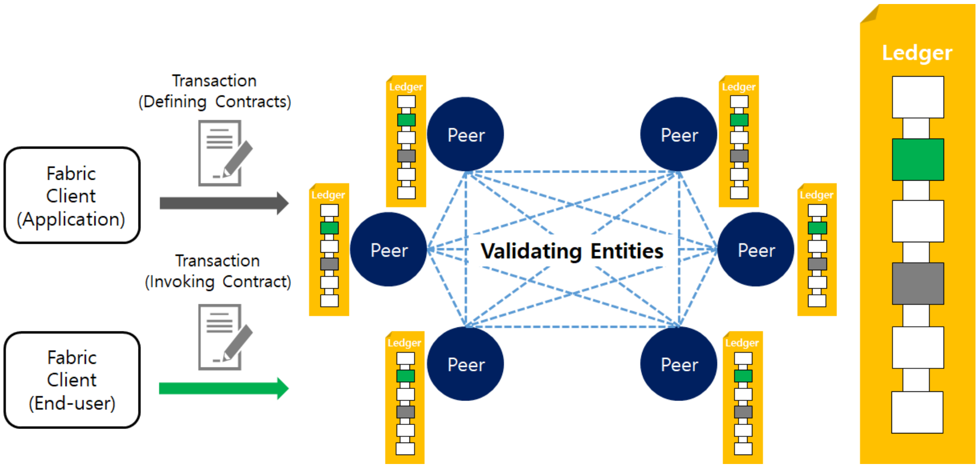


Figure 1. Hyperledger fabric model architecture

Since the proposed personal portfolio multilateral authentication system consists of a consortium of several institutions, it was implemented based on Hyperledger Fabric that is a consortium blockchain framework that allows only authorized institutions to participate in the network.

3. Proposed multilateral authentication system for personal portfolio

The personal portfolio multilateral authentication system proposed in this paper overcomes the problems of the existing educational administration information system consisting of a centralized system and uses blockchain technology to increase transparency and reliability in managing, storing, and distributing learner's learning history data. Personal Portfolio The personal portfolio of the multiparty authentication system contains the learner's ID, name, email, and training data. The process of the system is shown in [Figure 2].

Learner delivers learning data to peers configured in the Hyperledger Fabric network to perform identity authentication, registration, and evaluation. When the learner delivers a transaction to update the training data, the block is created by verifying the order and contents of the transaction by executing the chaincode installed in the peer and through the multi-factor authentication of all peers participating in the channel [9].

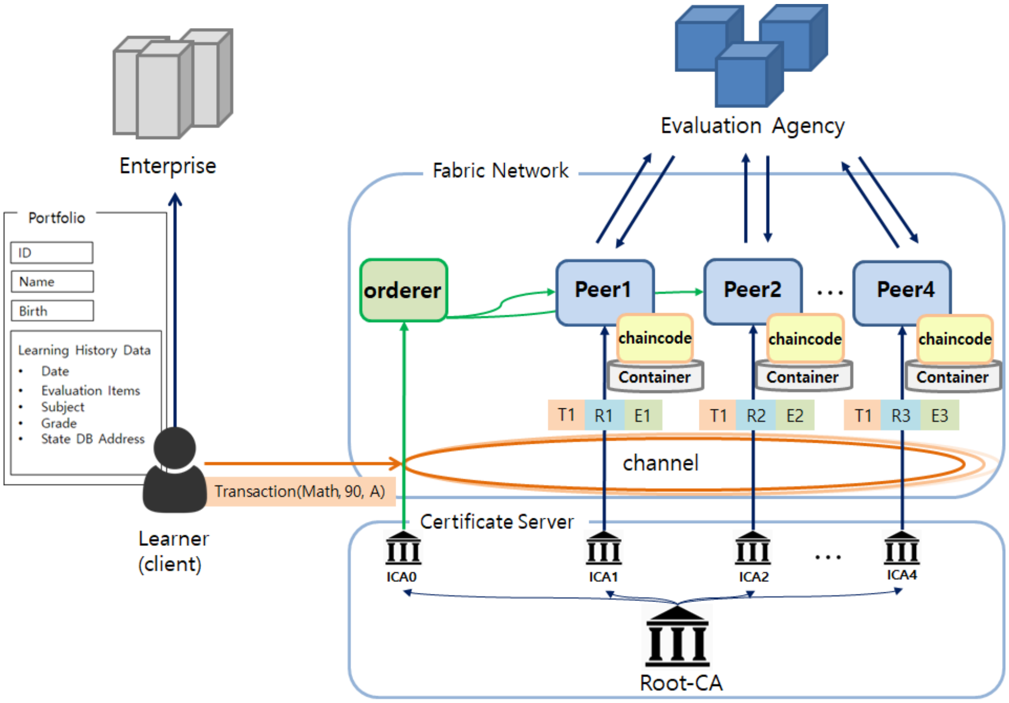


Figure 2. Personal portfolios multilateral authentication system

After the block is created, the learner can manage the portfolio directly by providing the key value and the evaluation data for the evaluation item to pass the completed training data back to the learner, but once the evaluation is completed and the block is generated, the learner It is not possible to directly modify and delete the training data. Therefore, the generated and linked blocks are authenticated data that cannot be modified and deleted, and because of the technical characteristics of the blockchain, transactions and blocks are stored and shared in all peers, thereby improving transparency and reliability.

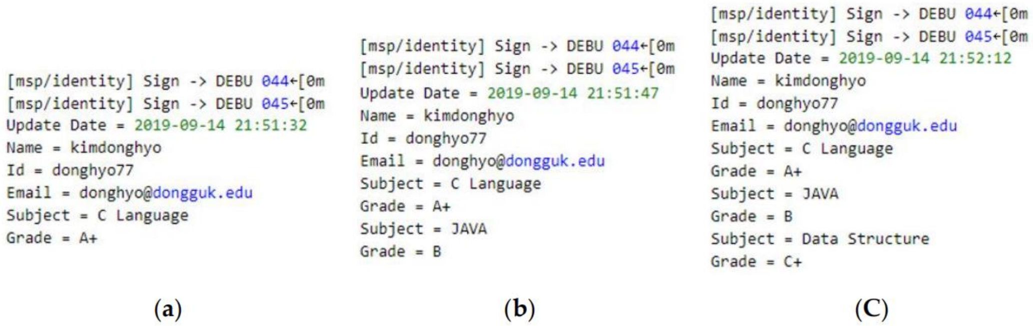
4. System implementation

In this paper, we implemented blockchain network and certification authority server by using Hyperledger Fabric and Docker platform and created Go language-based chaincode to implement personal portfolio multilateral authentication system. The environments for implementing Hyperledger Fabric blockchain network and certificate authority servers are Ubuntu v16.04 LTS, Hyperledger Fabric v1.2, Golang v11.4, Docker v18.06.1-ce, Docker-Compose v1.8.0, Nodejs v8. 11 and so on.

The authentication server generates encryption data such as each digital certificate and public key, private key, Genesis block, transaction generator, etc. in the peers and orderers belonging to the membership service. Based on this, the network is activated by containerizing the peers and orderers of the network, and when the network participants submit transactions, the chaincode installed on the peers is executed.

In order to record the transactions recorded in the ledger of the peer in the ledger of all peers, the transaction initialization request that records the learner's personal information and the learning history information is first transmitted, and the information is stored in the ledger by executing the Init function. In addition, the peers periodically check each other's statuses using the Gossip Protocol and distribute the transactions stored in the ledger using the anchor peer transaction generator that connects the peers created in the authentication server.

Figure 3 shows the result of executing Invoke function by sending the transaction update request to the chaincode installed in the peer and updating and inquiring the transaction recorded in the ledger of all peers participating in the channel.



```
[msp/identity] Sign -> DEBU 044←[0m
[msp/identity] Sign -> DEBU 045←[0m
Update Date = 2019-09-14 21:51:32
Name = kimdonghyo
Id = donghyo77
Email = donghyo@dongguk.edu
Subject = C Language
Grade = A+
```

(a)

```
[msp/identity] Sign -> DEBU 044←[0m
[msp/identity] Sign -> DEBU 045←[0m
Update Date = 2019-09-14 21:51:47
Name = kimdonghyo
Id = donghyo77
Email = donghyo@dongguk.edu
Subject = C Language
Grade = A+
Subject = JAVA
Grade = B
```

(b)

```
[msp/identity] Sign -> DEBU 044←[0m
[msp/identity] Sign -> DEBU 045←[0m
Update Date = 2019-09-14 21:52:12
Name = kimdonghyo
Id = donghyo77
Email = donghyo@dongguk.edu
Subject = C Language
Grade = A+
Subject = JAVA
Grade = B
Subject = Data Structure
Grade = C+
```

(C)

(a) update first transaction, (b) update second transaction, (c) update third transaction

Figure 3. A transaction that adds learning Information to the ledger by performing an invoke function

5. Conclusions

In this paper, we propose a personal portfolio multi-factor authentication system that can manage education-related data through a distributed ledger without a central authority based on transparency and reliability using blockchain technology.

For the implementation of the system, the network and authentication server of the personal portfolio multi-factor authentication system was built using the Hyperledger Fabric framework for building blockchain network infrastructure and Docker, a software virtualization platform. In addition, when registering and updating learning information with the configured peer, the chaincode is stored in the ledger of all peers participating in the channel, and a block is generated.

The system proposed in the paper can create a block so that once recorded learning data cannot be modified and deleted, and it is shared with all peers in the blockchain network, thus improving transparency and reliability, and it is expected that the problems of the existing learner information management system can be solved.

Acknowledgements

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (No.2017R1C1B5018257), and this research was supported by the Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education(No.2017R1D1A3B03029906), and this work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea Government (MSIT) (No.2018R1A5A7023490).

References

[1] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," Proceedings of IEEE 6th International Congress on Big Data, June 25-30, Hawaii, Unite State America, **(2017)** DOI: 10.1109/BigDataCongress.2017.85

[2] N. Satoshi, "Bitcoin: A peer-to-peer electronic cash system," http://www. bitcoin.org/bitcoin.pdf, **(2008)**

[3] M. Kim, S. Oh, and C. Hong, "Digital trading system using Hyperledger fabric block open source," Proceedings of Korea Computer Congress 2018, June 20-22, Jeju, Republic of Korea, **(2018)**

[4] C. Park, M. Kim, and H. Kim, "A study on building blockchain network and decentralized application development based on Hyperledger Fabric," Proceedings of Symposium of the Korean Institute of Communications and Information Sciences, June 20-22, Jeju, Republic of Korea, **(2018)**

[5] M. Lyu and M. Park, "A study on the methods of fault analysis for security improvement of national education information system (NEIS)," Journal of Korea Multimedia Society, vol.20, no.12, pp.1970-1979, **(2017)** DOI:10.9717/kmms.2017.20.12.1970

[6] L. S. Sankar, M.Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," Proceedings of 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), January 1-7, Coimbatore, India, **(2017)** DOI: 10.1109/ICACCS.2017.8014672

[7] J. Lee, "A docker container case study for implementing blockchain distributed general ledger," Korean Association of Computer and Accounting Review, vol.16, no.1, **(2018)**

[8] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, C. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. Weed Cocc, and J. Yellick, "Hyperledger fabric: A distributed operating System for permissioned blockchains," Proceedings of the 13th EuroSys Conference, April 23-26, Porto, Portugal, pp.1-15, **(2018)** DOI:10.1145/3190508.3190538

[9] Y. Hao, Y. Li, X. Dong, L. Fang, and P. Chen, "Performance analysis of consensus algorithm in private blockchain," Proceedings of IEEE Intelligent Vehicles Symposium, June 16-30, Suzhou, China, **(2018)** DOI: 10.1109/IVS.2018.8500557

Authors

Junho Jeong

He received the B.S. degree from the Dept. of Computer Science and Engineering, Dongguk University, Seoul, Korea, in 2007, and M.S. and Ph.D. degrees from the Dept. of Computer Science and Engineering, Dongguk University, Seoul, Korea in 2009 and 2015, respectively. He was a research professor of Electronic Commerce Institute, Dongguk University, Gyeongju, Korea from 2015-2019. And he was a research professor of Dept. of Computer Science and Engineering, Dongguk University, Seoul, Korea until 2019 Aug. Currently, he is an assistant professor of the Dept. of Computer Science and Engineering, Kongju National University, Cheonan, Korea. His research areas include Computer Security, Privacy Preserving, Distributed System, Network Security and Secure Software.

Donghyo Kim

He received Bachelor's degree in School of Computer Science and Engineering from Dongguk Computer Science Institute in 2017. Also, currently he is a master student in Dept. of Computer Science and Engineering, Dongguk University, Seoul. His current research interests include Blockchain, Smart Contract Security and Software Security.

Yangsun Lee

He received the B.S. degree from the Dept. of Computer Science, Dongguk University, Seoul, Korea, in 1985, and M.S. and Ph.D. degrees from Dept. of Computer Engineering, Dongguk University, Seoul, Korea in 1987 and 2003, respectively. He was a Manager of the Computer Center, Seokyeong University from 1996-2000, a Director of Korea Multimedia Society from 2004-2018, a General Director of Korea Multimedia Society from 2005-2006, a Vice President of Korea Multimedia Society in 2009, and a Senior Vice President of Korea Multimedia Society in 2015. Also, he was a Director of Korea Information Processing Society from 2006-2014 and a President of a Society for the Study of Game at Korea Information Processing Society from 2006-2010. And, he was a Director of HSST from 2014-2018. Currently, he is a Professor of Dept. of Computer Engineering, Seokyeong University, Seoul, Korea. His research areas include smart system solutions, programming languages, and embedded systems.

Yunsik Son

He received the B.S. degree from the Dept. of Computer Science and Engineering, Dongguk University, Seoul, Korea, in 2004, and M.S. and Ph.D. degrees from the Dept. of Computer Science and Engineering, Dongguk University, Seoul, Korea in 2006 and 2009, respectively. He was a research professor of Dept. of Brain and Cognitive Engineering, Korea University, Seoul, Korea from 2015-2016. Currently, he is an assistant professor of the Dept. of Computer Science and Engineering, Dongguk University, Seoul, Korea. Also, His research areas include secure software, programming languages, compiler construction, and mobile/embedded systems

This page is empty by intention.