

EUNICERT: ETHEREUM BASED DIGITAL CERTIFICATE VERIFICATION SYSTEM

Trong Thua Huynh¹, Dang-Khoa Pham²

¹Posts and Telecommunications Institute of Technology, Hochiminh city, Vietnam

²FPT Telecom, Hochiminh city, Vietnam

ABSTRACT

The fake certificate is a special global problem in today's digital age. Thousands of universities and educational institutions around the world do not exist but can release hundreds of millions of fake degrees. Verifying the integrity of qualifications is a real challenge for today's employers. Applying the anti-data modifying properties of blockchain technology, this study proposes a solution issuing and verifying digital certificates called EUniCert to solve this problem. By changing the design and integrating new consensus algorithm used in Ethereum platform into the Ucoin network that was used to verify and store the information related to the issued digital certificate, the EUniCert improves the latency to validate transactions as well as the number of verified blocks in the blockchain network compared to the previous solution that we have proposed. We implement a simple blockchain system to illustrate the management operation of the digital certificates on the ethereum platform. Besides, we conduct a simulation to evaluate the performance of our proposal compared with the previous system. The result is that the average latency decreases by 3.27 times as well as the number of verified blocks increases by 11% compared with the previous system.

Keywords

A Digital certificate, blockchain, ethereum, verification, counterfeit.

1. INTRODUCTION

Today, in a large and global labor market, certificates are used to assess the candidates' knowledge and skills. Unfortunately, this has increased the problem of counterfeiting, not only in underdeveloped countries but also as a truly global problem. In 2017, World Education Services estimates that there are more than 2,600 mills in operations globally and more than 1,000 in the United States. An estimated 400 of those in the U.S. award fake Ph.Ds [1]. Reported in "Global Study on Occupational Fraud and Abuse" in 2018 of the Association of Certified Fraud Examiners, there is a total of 2,690 real cases of occupational fraud from 125 countries in 23 industry categories [2].

In each country, there is a certificate authority certified by reputable organizations. However, these organizations cannot work to produce accurate results that have both objective and subjective factors. Moreover, the diversification of the industry and the broad demand of the labor market also create opportunities for many organizations to be established to issue certificates only to those who do not meet the required quality.

Currently, some universities around the world have adopted several techniques to create their services to issue and verify digital certificates such as [3], [4]. The verification can be automated by including the identity of the certificate into a central database, which can be accessed by a

company wishing to verify the credentials. However, this process has no unified mechanisms or standards in place such as a public registry, that is maintained by multiple institutions and accessible to everyone. On the contrary, the blockchain-based certificates are more simple to be issued and verified against a central database maintaining these certificates, and their security relies on available security cryptographic protocols.

Blockchain technology [5] is the backbone of modern cryptocurrencies such as Bitcoin, Ethereum. It is the simple mechanism providing state of the art distributed database systems with transparency, availability for data retrieval with security and privacy. Based on modern consensus techniques, systems based on blockchain have absolute resistance to data modification. This is highly applicable in digital certificate management systems to ensure that certificates are tamper-proof.

In recent years, there have been works [6], [7], [8], [9], [10], [11], [12] using blockchain technology to create a standardized platform for issuing and verifying digital certificates. Besides, in our recently published study [13], we have proposed and implemented an issuing and verifying system called UniCert based on the Unicoins network which is a digital currency built on blockchain technology using the power of work consensus algorithm [14]. In this study, we improve the latency to validate transactions as well as the number of verified blocks in the blockchain network. To do this, we have focused on changing the design and integrating the new consensus algorithm used in the Ethereum platform into the Unicoins network that was used to verify and store the information related to the issued digital certificate.

The remainder of the paper is organized as follows. In section 2, we present the related works. Section 3 describes the architecture of the system inherited from our previous study. Section 4 describes the design and implement of the block validating algorithm as well as new classes in the EUnicoins blockchain. Section 5 evaluates the results of the improved system compared to the previous system. Finally, concluding remarks are given in section 6.

2. RELATED WORKS

By providing reliable, decentralized and public data storage, blockchain has become a breakthrough technology that receives interest from many application areas. Many attempts have been made to extend the usage of blockchain technology to solve the counterfeit certification issue in education [15].

Mozilla Open Badges [16] and BADGR [17], both offers unified solutions to manage the entire educational history of students by collating all the digital certificates they have obtained at different academies and link it with a unique identity. Although these solutions do not use blockchain, they show how to integrate multiple certificates into the student identity.

The goal of blockchain in the field of education is to create a digital certificate into a piece of automatically verifiable information that third parties can refer to through a constant system of evidence. According to [18], blockchain can be deployed in two separate ways in the field of education. Although the first requires that the certificates are stored in plain text to create a public database, the second requires only storing the hash of the certificate to ensure the digital certificate is given to students. Therefore, published student data can be seen by anyone, because they do not contain any confidential information. Because certificates are required to be counterfeit, it is appropriate to use blockchain as decentralized storage.

The first notable use case storing a hash of certificates is Blockcerts [9], an application based on blockchain technology and aligned with the open badge ecosystem [11]. With transparency and

availability provided by the blockchain network, Blockcerts serves as a middleware for issuing and retrieving certificates online. The stored certificates are accessible via a wallet, which enables employees to get a verifiable, tamper-proof version of their certificate which they can share with employers and other organizations. However, Blockcerts has its drawbacks. By connecting to the Bitcoin network, Blockcerts ties itself to the Bitcoin market at fluctuating rates which makes the requirements for issuing certificate unpredictable. Moreover, the Bitcoin network keeps getting bigger, this results in an expensive fee for the new node to join the network.

Similar to Blockcerts's approach, the Greek National Education and Research Network (GRNET) [8] is also storing a single blockchain certificate hash to protect student confidential data. The goal is to create a system that can verify student certificates on the Cardano blockchain reducing manual verification and fake certificate cases. However, the GRNET [8] project differs from Blockcerts [9] in the sense that it can store not only certificate hashes but also the entire verification process. Request verification, proof of success or failure and forward the results to the requester that the steps will be stored.

There is a little difference, Oxcert [10] creates a private blockchain with different currency types in the network which amplifies usage of blockchain. This private blockchain separates common usage of the transaction and the process of certification. Therefore, the certification fee becomes stable due to the non-fungible tokens. Besides, some projects with similar functionalities have been deployed as web services such as Open Certificates [11] and CertChain [12]. Open Certificates allows us to start issuing certificates and badges easily using our hosted web application. We can also integrate it into our infrastructure using our APIs. Meanwhile, CertChain is the quality certification service based on blockchain technology to keep, search, monitor and share certificates safely and user-friendly.

BCDiploma [6], EduCTX [19] and UNIC (University of Nicosia) [20] have started projects based on blockchain technology to issue and verify certificates. BCDiploma and EduCTX have a common goal towards a global certification network of higher academic institutions. Meanwhile, UNIC intends to convert its internal processes into a distributed system that issues digital certificates. Although these methods are full-blown, they do not meet the practical requirements or are hard to integrate into the structure of the education institution.

3. SYSTEM ARCHITECTURE – EUNICERT

3.1. Principle of Operation

The operating principle of the system is inherited from our recent study [13] and the improved consensus algorithm. Overcoming the disadvantages of the PoW [14] consensus mechanism requiring nodes to participate in calculation to solve hash functions that take a lot of time and energy, we improve the architecture by integrating PoS consensus mechanism which the verifier the next block is selected via the combination of random selection and his stake into blockchain network to change the method of the block packaging. Accordingly, among participating nodes, a node will be selected base on the stake value to become a block verifier. This node is called a validator. The condition to participate in this process is that these nodes need to put a certain amount of money into the network to place a bet. This money is called a stake. This money will be locked and will be unlocked after the node withdraws from participating in the validator after a while. The selected validator will verify the block and append it to the blockchain. If the block is valid and entered into the chain, this validator will be rewarded from the transaction fee.

In addition to saving energy consumption and time to solve hash values, stake-based consensus mechanisms also make the system more difficult to attack than computing power-based

consensus mechanisms. If the attack fails, the attacker will be penalized for losing his entire bet amount. Specifically, to perform a 51% attack, an attacker needs to have more than 50% of the system's coins, which is even more unlikely when the total market value of Ethereum has now reached more than 30 billion USD [21].

3.2. EUniCert Architecture

As shown in Figure 1, users interact with the system through EUniCert Frontend to use web services. EUniCert Backend connects to EUniCoin system to issue certificates into the EUniCoin Network which creates transactions and puts them into the block. All the processes such as issuing, retrieving and verifying are provided in EUniCert Frontend.

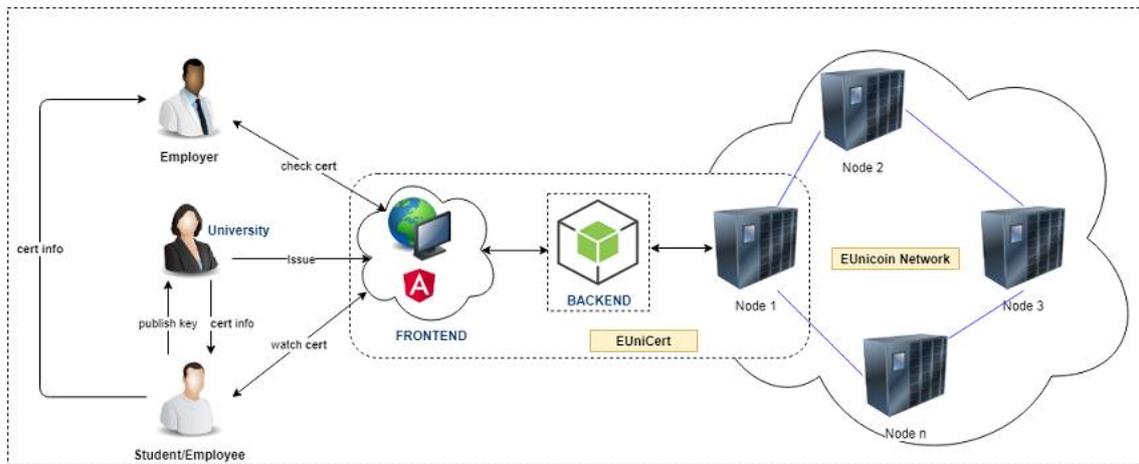


Figure 1. EUniCert Architecture

4. IMPLEMENTING EUNICERT BLOCKCHAIN

4.1. Implementing EUniCoin Network

The block validating process in EUniCoin network is carried out according to the algorithm as shown in Figure 2, including the following main steps:

- i. In the network, If a node wants to become a validator, it will first pay the validating fee
- ii. When the transaction is confirmed, then it can deposit some coins (stakes) to compete with other validators
- iii. Meanwhile, each node is responsible for distributing the transactions they receive from clients.
- iv. When a sufficient amount of transactions are created, the validators select a leader with the largest staked coins. The selected leader then creates a block and distributes it to the network.
- v. Each node verifies the block, executes all the transactions in the block and appends the block in the blockchain.
- vi. The block also has a special transaction as a reward. The leader for the given round gets the transaction fees of the transactions presented in the block as a reward.

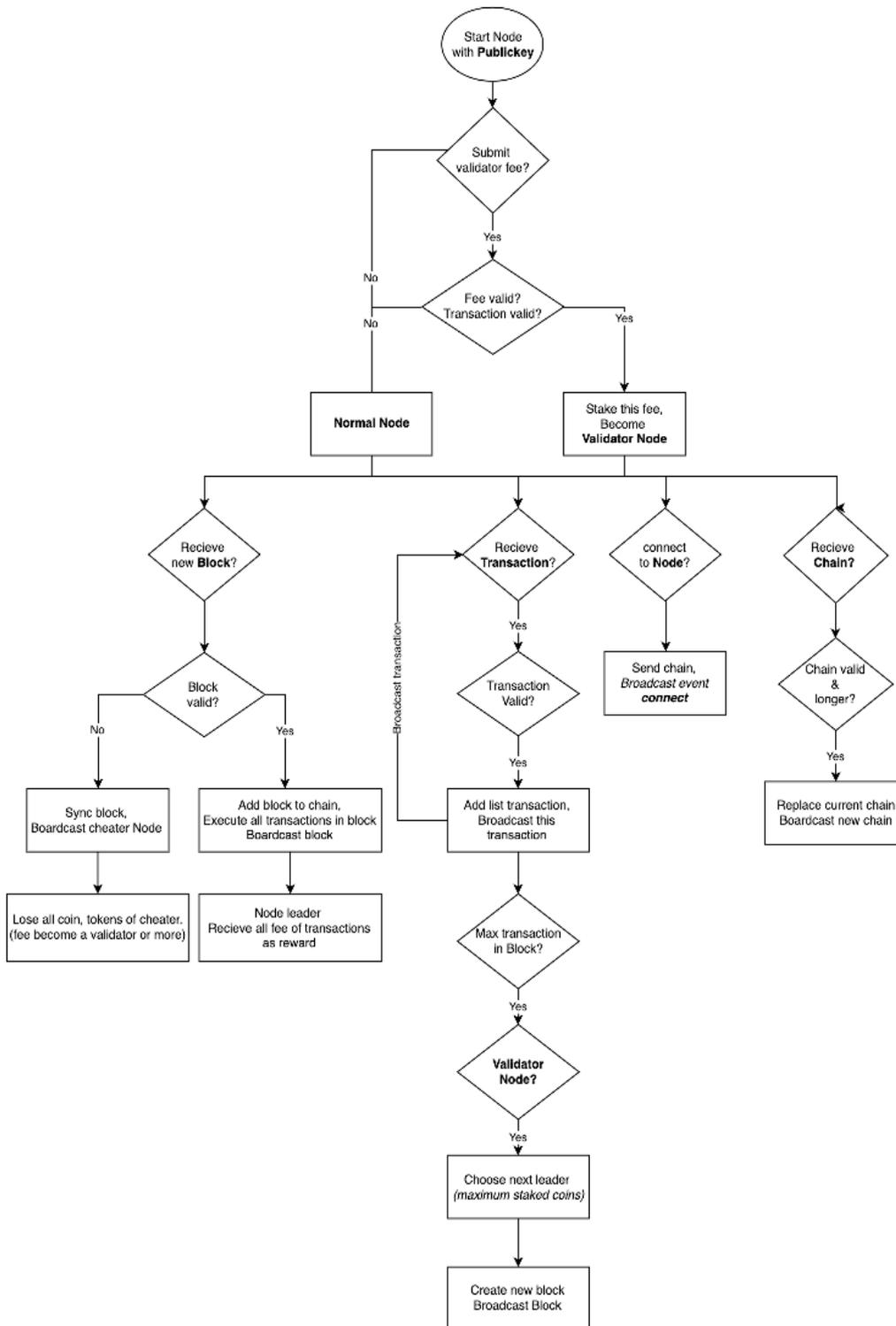


Figure 2. Algorithm to validate block into the blockchain

4.2. Classes Design

The class designs of the EUniCert module (in Figure 1) are reused from the UniCert system in our recent study [13]. This section presents the designs in the EUnicoin blockchain module.

a) The blockchain classes described in Figure 3 include the following classes:

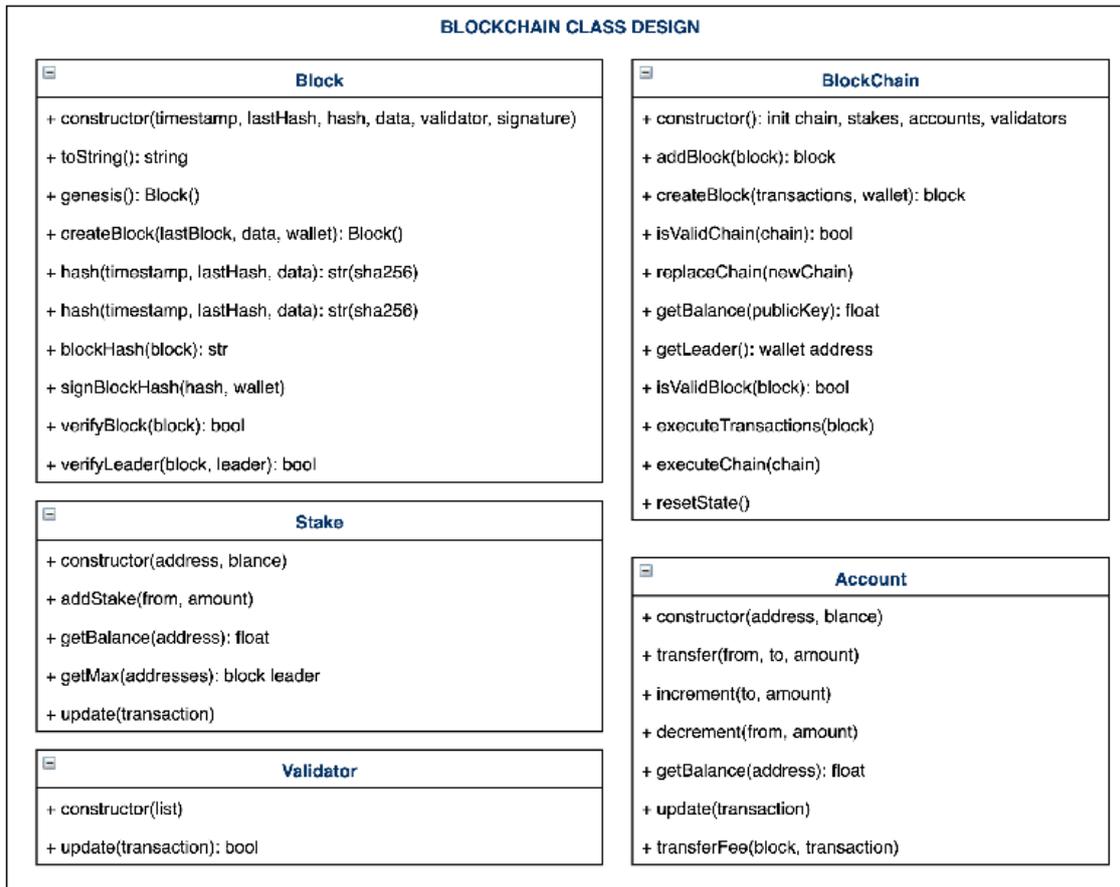


Figure 3. Classes Design for EUnicoin Blockchain

- **Block class:** Blockchain is made of blocks. Class for each block has the following properties:

- timestamp: the time of the creation of block in milliseconds.
- lastHash: the hash value of the last block on the chain.
- hash: the hash value of the current block.
- data: data in the block or transactions.
- validator: the address of the node that made this block.
- signature: the encrypted hash of the block, signed by the validator.

```

class Block {
    constructor(timestamp, lastHash, hash, data, validator,
signature) {
        this.timestamp = timestamp;
        this.lastHash = lastHash;
        this.hash = hash;
    }
}
    
```

```
        this.data = data;
        this.validator = validator;
        this.signature = signature;
    }
}
```

- **Blockchain class:** manages information in the blockchain network.

```
class Blockchain {
    constructor() {
        this.chain = [Block.genesis()];
        this.stakes = new Stake();
        this.accounts = new Account();
        this.validators = new Validators();
    }
}
```

- **Account Model:** We use an account model to track node balances. This model is another Merkle tree in Ethereum as a blockchain. Each transaction when executed will increase the balance for a specific account or reduce that balance. Therefore, it can be considered simply a key-value hash table in which the key is the account of the nodes and the value is the balance. Instead of creating a Merkle tree, we will only create an object in our application to create the account model
- **Validator class:** Validator nodes are different from normal nodes. These nodes can add stake, be selected as a leader and create new blocks. But not all nodes can be a validator. Only those nodes that send the special transaction with a validating fee can become a validator. The fee or coins are later burnt and not used.
- **Stake Model:** We need a way to track the number of coins a node has staked. In the Ethereum platform, each block keeps the amount of staked coins and create a separate model for it. Since the node with the largest stake is selected as the leader, we find the next leader by searching for the staked coins in this model. The functionality of the stake model will be similar to the account model.

b) Wallet and P2P classes described in Figure 4 include the following classes:

- **Transaction class:** Our transactions have the following structure:

```
id: <here goes some identifier>
type: <transactions type: stake,validator,transaction>
input: {
    timestamp: <time of creation>,
    from: <senders address>,
    signature: <signature of the transaction>
}
output: {
    to: <recievers address>
    amount: <amount transfered>
    fee: <transactions fee>
}
class Transaction {
    constructor() {
        this.id = ChainUtil.id();
        this.type = null;
        this.input = null;
        this.output = null;
    }
}
```

```
}
}
```

- **Transaction pool:** Because many individuals who make transactions with their wallets on cryptocurrency will need a way to include groups of these transactions, we use the concept of the transaction pool. The transaction pool will be an updated real-time object containing all new transactions sent by all network miners.
- **Wallet:** manages information related to wallet address information in the system: increase or decrease balance, available balance, etc.
- **P2P Server:** used for distributing the interactive data to nodes in the network. It operates follow the rules of written code.

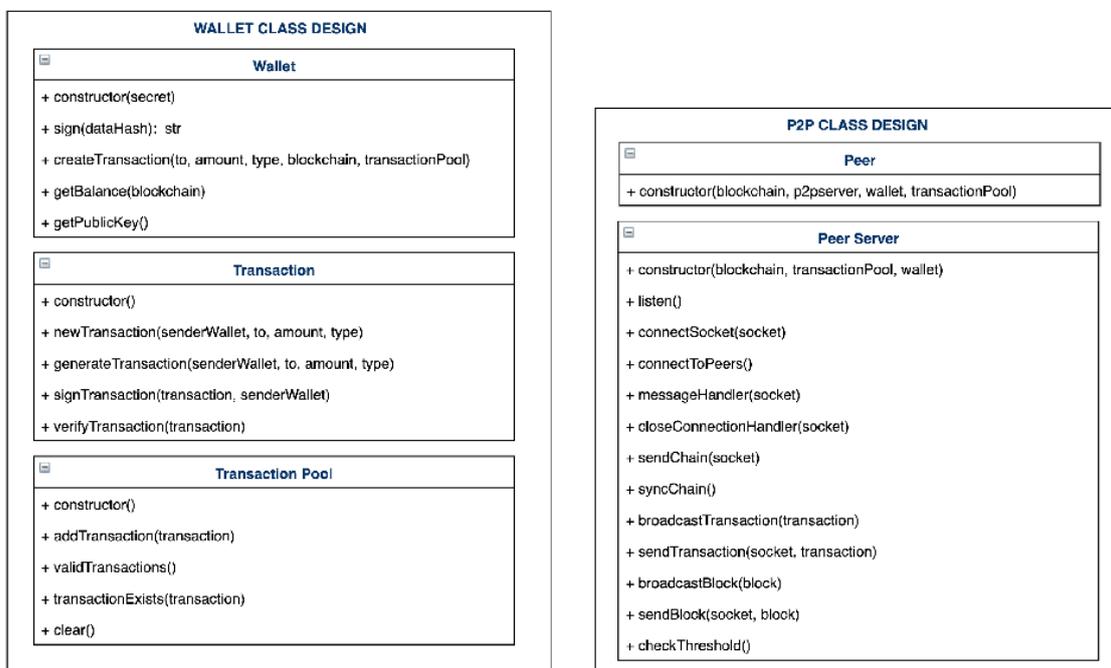


Figure 4. Classes Design for Wallet and P2P protocol

5. RESULT EVALUATION

We have built a simple EUniCert system to illustrate the management operation of the digital certificates on the Ethereum blockchain. For the certificate issuing, as shown in Figure 5, the required information of the issuer is for charging a fee under his EUniCoin address. Issuer’s organization logo, name, emails are for uniqueness and the URL is for more trust.

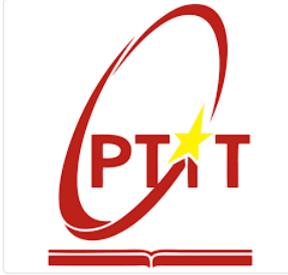
Issuer Information	
ID / PubKey	f484a3b4239345329da836ad80248e71
Logo	
Name	PTIT HCM
Url	http://portal.ptit.edu.vn/
Email	ptithcm@edu.vn

Figure 5. Information of Issuer

As shown in Figure 6, the main content contains detailed information about the certificate issued to a particular recipient.

Main Content
ID Recipient: uuid:4de1a96a-3501-46ed-8f75-49612bbac257
Issue For: Join Son
Email Recipient: joinson@gmail.com
Degree Class: Good
Description: Lorem ipsum dolor sit amet, mei docendi concludaturque ad, cu expetenda moderatius neglegentur ei nam, suas dolor laudem eam an.

Figure 6. Detail Information of Certificate.

In addition to the above results after implementing the EUniCert system, we conducted simulation-based on WRK [22], a modern HTTP benchmarking tool, with 12 threads and 1000 connections to evaluate the performance of the UniCert system [13] and our proposed improvement EUniCert based on the average latency for performing the block validation as well as the number of verified blocks into the blockchain.

In Table 1, we changed the timeout parameter to evaluate the system performance according to the service quality required by the system based on the average latency to validate the block into the blockchain network.

With the timeout limit set to 1 second, the average latency of this proposal (EUniCert) increases compared to the old system (UniCert). However, with the timeout limit set from 2 to 4 seconds, the effect increases markedly. Specifically, with the timeout limit set to 3 seconds, the average latency is decreased by 661.10 milliseconds, corresponding to the gain ratio of 3.27 times compared to our previous system.

Table 1. Average Latency to validate the block

Timeout limit (s)	UniCert (ms)	EUniCert (ms)	Difference (ms)	Gain Ratio
1	403.43	409.76	-6.33	0.98
2	753.3	270.71	482.59	2.78
3	952.41	291.31	661.10	3.27
4	989.23	329.61	659.62	3.00

In Table 2, we changed the timeout limit parameter to evaluate the system performance according to the service quality required by the system based on the number of timeout requests that are not processed by the blockchain network.

By setting the timeout limit to 1 second, the number of timeout requests received by this proposal is significantly reduced (1358 requests) compared to the old system (UniCert). However, the highest gain ratio is 4.07 times with timeout limit is set to 2 seconds. Meanwhile, with the timeout limit set to 3 seconds, the gain ratio is only 2.14 times; 4 seconds is 2.44 times. Therefore, to balance between the two factors average latency and the number of timeout requests, we can choose the timeout limit in the range of 2 to 4 seconds.

Table 2. Number of timeout requests

Timeout limit (s)	UniCert (no. of req.)	EUniCert (no. of req.)	Difference (no. of req.)	Gain Ratio
1	1816	458	1358	3.97
2	766	188	578	4.07
3	392	183	209	2.14
4	154	63	91	2.44

In Table 3, we evaluate the number of blocks (requests) validated in the system according to the simulation intervals of 10, 30 and 60 seconds.

Table 3. Number of validated blocks (requests)

Duration (s)	Timeout Requests			Requests/sec		
	UniCert	EUniCert	Gain Ratio	UniCert	EUniCert	Gain Rate
10	1816	458	3.97	284.71	265.13	93%
30	9609	2476	3.88	505.67	559.21	111%
60	20135	5668	3.55	530.46	571.52	108%

When the duration simulation is set to 10 seconds, the gain ratio on the number of timeout requests is the best with 3.97 times but the gain rate on the number of validated requests (blocks) is only 93%. While for 30 seconds (duration), both the gain ratio on timeout requests and the gain rate on validated requests are 3.88 times and 111%, respectively. Therefore, to improve the efficiency of block validation in this simulation, the proposed parameter for the duration is 30 seconds.

6. CONCLUSIONS

Based on the results of our previous study and the superior consensus algorithm in the Ethereum platform, we have proposed the EUniCert to improve the performance of transaction verification in the digital issuing and validating system on the blockchain platform. We have also designed new classes in the improved system (EUniCert) and implemented a system to evaluate the performance compared to the previous system (UniCert). Evaluation results showed an appreciable reduction in the average latency to validate blocks and a significant increase in the number of verified blocks in the blockchain. In this study, we implemented the PoS consensus algorithm based on the Casper protocol. In the future study, we will implement Casper version 2 and apply smart contracts to create digital certificates for improving security and transparency.

REFERENCES

- [1] Hanna Park & Ashley Craddock, (2017) "*Diploma Mills: 9 Strategies for Tackling One of Higher Education's Most Wicked Problems*", [Online], Available: <https://wenr.wes.org/2017/12/diploma-mills-9-strategies-for-tackling-one-of-higher-educations-most-wicked-problems>.
- [2] Bruce Dorris, J.D, (2018) "*Report to the Nations, Global study on occupational fraud and abuse*", Association of Certified Fraud Examiners.
- [3] My eQuals, (2017), "*The Official Platform of Australian and New Zealand Universities*", [Online], Available: <https://www.myequals.edu.au/>
- [4] Mozilla, (2018), "*Open Badges*", [Online], Available: <https://openbadges.org/>
- [5] Michael Crosby, Nachiappan, Pradan Pattanayak, Sanjeev Verma & Vignesh Kalyanaraman, (2016), "*Blockchain Technology: Beyond Bitcoin*", Applied Innovation Review, no. 2.
- [6] BCDiploma, (2017), "*Degrees Certified on the Blockchain*", [Online], Available: <https://www.bcdiploma.com/index.html>
- [7] Elizabeth Durant & Alison Trachy, (2017), "*Digital Diploma debuts at MIT*", [Online], Available: <http://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017>
- [8] Amy Castor, (2018), "*Cardano Blockchain's First Use Case: Proof of University Diplomas in Greece*", [Online], Available: <https://bitcoinmagazine.com/articles/cardano-blockchains-first-use-case-proof-university-diplomas-greece>
- [9] Blockcert, [Online], Available: <https://www.blockcerts.org>
- [10] Kristijan Sedlak & Jure Zih, "0xcert protocol", [Online], Available: <https://0xproject.com>
- [11] Open Certificates, [Online], Available: <http://opencertificates.co>
- [12] CertChain, [Online], Available: <https://certchain.io>
- [13] Trong Thua Huynh, Trung Tru Huynh, Dang Khoa Pham & Anh Khoa Ngo, (2018), "*Issuing and Verifying Digital Certificates with Blockchain*", International Conference on Advanced Technologies for Communications, IEEE, p.332-336.
- [14] Ben Laurie , Richard Clayton, (2004), "*Proof-of-Work proves not to work; version 0.2*", in Workshop on Economics and Information Security.

- [15] Wolfgang Gräther et al., (2018), "*Blockchain for Education: Lifelong Learning Passport*" in ERCIM-Blockchain Workshop.
- [16] Mozilla Foundation, Peer 2 Peer University & MacArthur Foundation, (2012), "*Open Badges for Lifelong Learning*", Working Document.
- [17] Badgr.io: Make your badges meaningful with Badgr (2018), [Online], Available: <https://badgr.com/>
- [18] Grech, A. and Camilleri, A.F., (2017), "Blockchain in Education", Technical report.
- [19] Muhamed Turkanović, Marko Hölbl, Kristjan Košič, Marjan Heričko & Aida Kamišalić, (2018), "EduCTX: A Blockchain-based Higher Education Credit Platform. IEEE Access.
- [20] University of Nicosia, (2018), "*Academic Certificates on the Blockchain*", [Online], Available: <https://www.unic.ac.cy/blockchain/free-mooc/>
- [21] Top 100 Cryptocurrencies by Market Capitalization, [Online], Available: <https://coinmarketcap.com/>
- [22] wrk - a HTTP benchmarking tool, [Online], Available: <https://github.com/wg/wrk>

AUTHORS

Trong Thua Huynh is currently the Head of Information Security Department, Faculty of Information Technology, Posts and Telecommunications Institute of Technology in Ho Chi Minh City, Vietnam. Trong Thua Huynh received a Bachelor's degree in Information Technology from Ho Chi Minh City University of Natural Sciences, a Master degree in Computer Engineering at Kyung Hee University, Korea and a Ph.D. degree in Computer Science at Ho Chi Minh City University of Technology, Vietnam National University at Ho Chi Minh City. His key areas of research include Information Security in IoT, Blockchain, Cryptography, and Digital Forensics.



Dang Khoa Pham is currently the Full Stack Developer, FPT Play - FPT Telecom in Ho Chi Minh City, Vietnam. Dang Khoa Pham received a Bachelor's degree in Information Technology from Posts and Telecommunications Institute of Technology in Ho Chi Minh City, Vietnam. His main research interests are Blockchain, Cryptography and Artificial Intelligence.

