Proceedings of IEEE International Conference on Applied System Innovation 2018
IEEE ICASI 2018- Meen, Prior & Lam (Eds)

Blockchain and Smart Contract for Digital Certificate

Jiin-Chiou Cheng[1], Narn-Yih Lee[2], Chien Chi[3], and Yi-Hua Chen[4]

[1,2,3]Department of Computer Science and Information Engineering,
Southern Taiwan University of Science and Technology, Tainan, Taiwan
[4]National Applied Research Laboratories, Natinal Center for High-Performance Computing
[1] chiou@mail.stust.edu.tw [2] nylee@mail.stust.edu.tw [3] 4a3g0052@stust.edu.tw [4] 1703154@nchc.narl.org.tw

Abstract

According to the Taiwan Ministry of Education statistics, about one million graduates each year, some of them will go to countries, high schools or tertiary institutions to continue to attend, and some will be ready to enter the workplace employment. During the course of study, the students' all kinds of excellent performance certificates, score transcripts, diplomas, etc., will become an important reference for admitting new schools or new works. As schools make various awards or diplomas, only the names of the schools and the students are input. Due to the lack of effective anti-forge mechanism, events that cause the graduation certificate to be forged often get noticed. In order to solve the problem of counterfeiting certificates, the digital certificate system based on blockchain technology would be proposed. By the unmodifiable property of blockchain, the digital certificate with anti-counterfeit and verifiability could be made. The procedure of issuing the digital certificate in this system is as follows. First, generate the electronic file of a paper certificate accompanying other related data into the database, meanwhile calculate the electronic file for its hash value. Finally, store the hash value into the block in the chain system. The system will create a related QR-code and inquiry string code to affix to the paper certificate. It will provide the demand unit to verify the authenticity of the paper certificate through mobile phone scanning or website inquiries. Through the unmodifiable properties of the blockchain, the system not only enhances the credibility of various paper-based certificates, but also electronically reduces the loss risks of various types of certificates.

Key words: blockchain, hyperledger, digital certificate, hashing.

Introduction

A. Background Information

Advances in information technology, the wide availability of the Internet, and common usage of mobile devices have changed the lifestyle of human beings. Virtual currency, digital coins originally designed for use online, has begun to be extensively adopted in real life. Because of the convenience of the Internet, various virtual currencies are thriving, including the most popular—Bitcoin, Ether, and Ripple [2]—the value of which has surged recently. People are beginning to pay attention to blockchain, the backbone technology of these revolutionary currencies. Blockchain features a decentralized and incorruptible database that has high potential for a diverse range of uses.

Blockchain is a distributed database that is widely used for recording distinct transactions. Once a consensus is reached among different nodes, the transaction is added to a block that already holds records of several transactions. Each block contains the hash value of its last counterpart for connection. All the blocks are connected and together they form a blockchain [1]. Data are distributed among various nodes (the distributed data storage) and are thus decentralized. Consequently, the nodes maintain the database together. Under blockchain, a block becomes validated only once it has been verified by multiple parties. Furthermore, the data in blocks cannot be modified arbitrarily. A blockchain-based smart contract, for example, creates a reliable system because it dispels doubts about information's veracity.

B. Rationale

Because information technology has developed rapidly in recent years, data protection is more necessary than ever. Graduates, whether they choose to continue studying or start job hunting, require various certificates for interviews. However, they often find that they have lost their educational and commendation certificates. Reapplying for hard copies can be time-consuming because certificates are granted by different organizations and in-person application may be necessary. By contrast, applying for an e-copy can save paper and time. By providing information for identity verification, graduates are able to apply for any certificate easily. Nevertheless, because of this convenience, forged degree certificates, licenses, and certificates are prevalent. Consequently, schools and companies cannot instantly validate the documents they receive [5]. To solve this problem, a certificate system based on blockchain was designed in this study. Data are stored in different nodes, and anyone who wishes to modify a particular internal datum must request that other nodes modify it simultaneously. Thus, the system is highly reliable.

C. Objectives

In this study, we developed a decentralized application and designed a certificate system based on Ethereum blockchain. This technology was selected because it is incorruptible, encrypted, and trackable and permits data synchronization. By integrating the features of blockchain, the system improves the efficiency operations at each stage. The system saves on paper, cuts management costs, prevents document forgery, and provides accurate and reliable information on digital certificates.

Literature Review

A. Blockchain

The concept of blockchain was proposed by Satoshi Nakamoto in 2008. Blockchain is an online ledger that provides decentralized and transparent data sharing. With distributed recordings, all transaction data (stored in nodes) are compressed and added to different blocks. Data of various

ISBN 978-1-5386-4342-6

types are distributed in distinct blocks, enabling verifications to be made without the use of intermediaries. All the nodes then form a blockchain with timestamps. The data stored in each block can be verified simultaneously and become inalterable once entered. The whole process is open to the public, transparent, and secure [8].

The emergence of Ethereum Smart Contracts in 2013 boosted blockchain technology, which became blockchain 2.0. As presented in Fig. 1, blockchain 1.0 was mainly adopted by Bitcoin to solve problems concerning cryptocurrencies and decentralized payments. Blockchain 2.0 focused on decentralizing the entire market and is employed to transform assets through smart contracts, thereby creating value through the emergence of alternatives to Bitcoin .

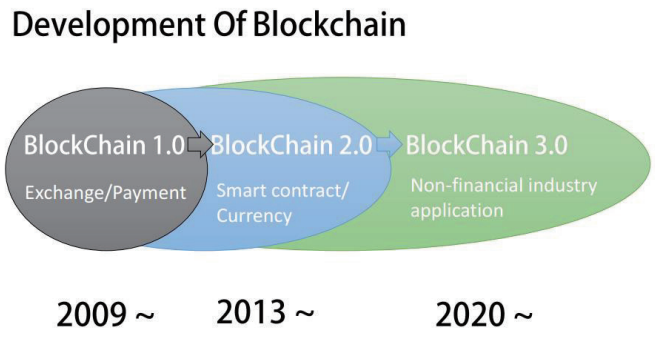

Fig. 1. Development of blockchain [9]

B. Ethereum

Ethereum is an open and decentralized platform featuring Turing completeness and supporting various derivative applications. Most smart contracts and decentralized autonomous organizations are created by using Ethereum [10]. If the Bitcoin blockchains are considered a global payment network, Ethereum would be the global computing system. Furthermore, Ethereum is an open-source platform similar to Android (developed by Google). It provides an infrastructure that enables developers to create applications. The infrastructure is developed and maintained by both Ethereum and those developers. The major characteristics of Ethereum are as follows:

1) incorruptible: third-parties are not able to modify any data;
2) secure: errors derived from personnel factors are avoided because the decentralized applications are maintained by entities rather than individuals;
3) permanent: blockchain does not cease to operate even if an individual computer or server crashes.

1) *Ethereum Virtual Machine (EVM)*

The EVM is a programmable blockchain. Unlike Bitcoin, which provides a fixed set of commands, the EVM allows developers to run any programs in the manner they wish. Developers instruct the EVM to execute applications by using a high-level language called Solidity [11].

2) *Solidity*

Solidity is the programing language used for implementing smart contracts and is similar to JavaScript. After a Solidity-programmed smart contract is completed, a complier called solc is required to transform the Solidity code into contract bytecode, which is then interpreted by the EVM. Next, the compiled instructions are deployed in an Ethereum blockchain. This completes the whole process (Fig. 2).

```
pragma solidity ^0.4.0;

contract SimpleStorage {
    uint storedData;

    function set(uint x) {
        storedData = x;
    }

    function get() constant returns (uint) {
        return storedData;
    }
}
```

Fig. 2. The Solidity program [13].

C. Smart Contracts

Smart contracts were first proposed by Nick Szabo in the early 1990s. He explained that a smart contract enabled computers to execute transaction clauses. As blockchain has become popular, smart contracts have received increased attention. Smart contracts are the main feature of Ethereum, a blockchain platform founded in 2015. A smart contract is "a digital contract that is written in source code and executed by computers, which integrates the tamper-proof mechanism of blockchain" [6]. Smart contracts can be created using the Ethereum blockchain. Developers are able, according to their needs, to specify any instruction in smart contracts; develop various types of applications, including those that interact with other contracts; store data; and transfer Ethers. Additionally, smart contracts that are deployed in blockchains are copied to each node to prevent contract tampering. With related operations executed by computers and services provided by Ethereum, human error can be reduced to avoid disputes regarding such contracts. Smart contracts are mostly used in voting system [7] and cryptocurrency applications. Fig. 3 depicts an example of how developers can easily deploy smart contracts for cryptocurrency transactions. The high-level programming languages used for writing smart contracts are mainly Solidity, Serpent, and LLL [12]. Currently, most developers employ Solidity to write smart contracts and compile the instructions into bytecode for the EVM to execute. Certain costs are incurred when developers create smart contracts.

Fig. 3. Uses of smart contracts.

Research Methods

A. System Design

In this study, a blockchain certificate system was

ISBN 978-1-5386-4342-6

developed based on relevant technology. The system's application was programmed on the Ethereum platform and is run by the EVM. In the system, three groups of users are involved, (Fig. 4). Schools or certification units grant certificates, have access to the system, and can browse the system database. When students fulfilled certain requirements, the authorities grant a certificate through the system. After the students have received their certificate, they are able to inquire about any certificate they have gained. The service provider is responsible for system maintenance.

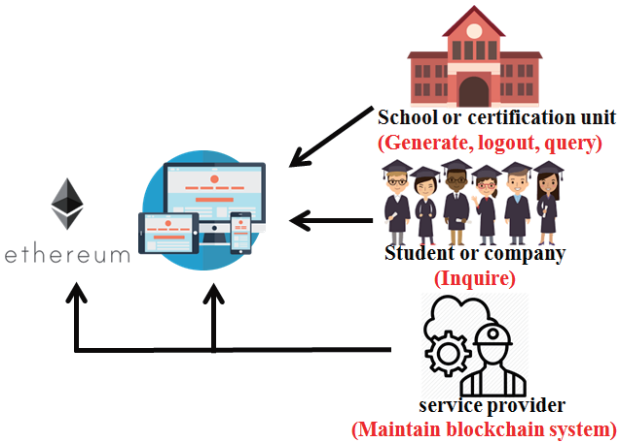

Fig. 4. Configuration of the blockchain-based system.

B. Process

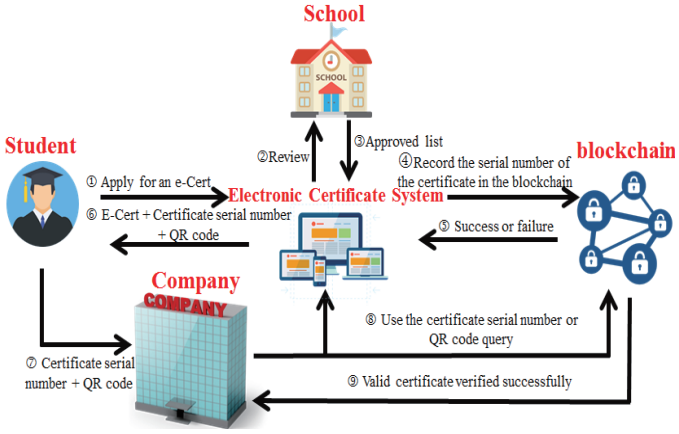

Fig. 5. Working process of the system.

Blockchain is a decentralized distributed database. The working processes of the system developed in this study are as follows:

1) Schools grant a degree certificate and enter the student's data into the system. Next, the system automatically records the serial number of the student in a blockchain.

2) The certificate system verifies all the data.

3) Instead of sending conventional hard copies, schools grant e-certificates containing a quick response (QR) code to the graduates whose data have been successfully verified. Each graduate also receives an inquiry number and electronic file of their certificate.

4) When applying for a job, a graduate simply sends the serial number or e-certificate with a QR code to the target companies.

5) The companies send inquiries to the system and are informed if the serial numbers are validated. The QR code enables them to recognize if the certificate has been tampered with or forged.

C. Operation

On the sign in page, the user clicks "register now," fills in their basic information, and receives a confirmation email (Figs. 6 and 7).

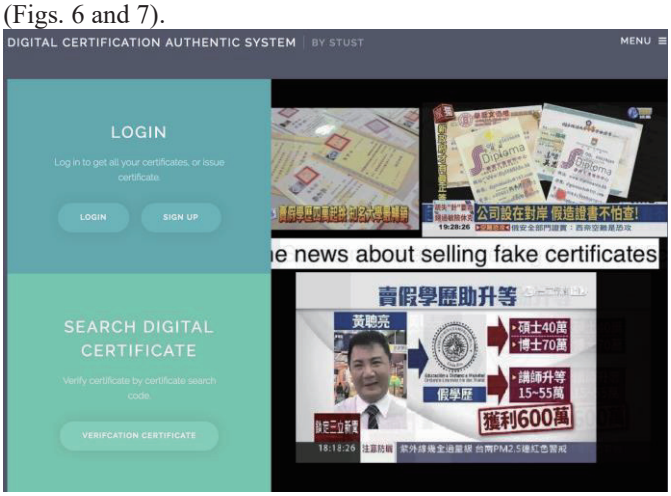

Fig. 6. Front page of the blockchain certificate system.

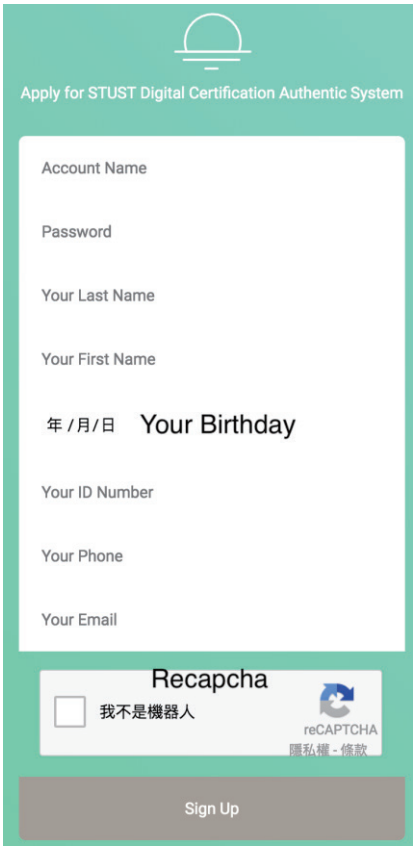

Fig. 7. Registration page.

1) *Certification Units*

ISBN 978-1-5386-4342-6

After certification units (i.e., schools) have entered the information of a graduate, the system creates an e-certificate containing a QR code and generates a serial number for the certificate. The data are then recorded in the blockchain. Next, the system sends a notification and inquiry number to the graduate for future inquiries (Figs. 8–11).

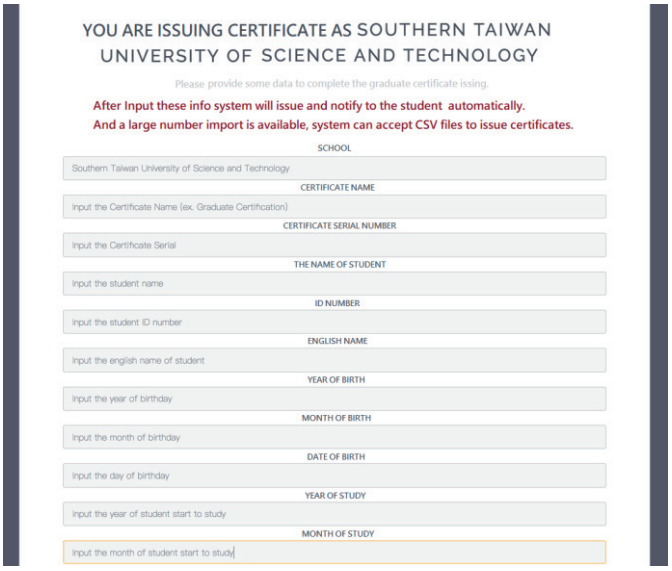

Fig. 8. Certification units complete the relevant information.

Fig. 9. Graduate receives a confirmation letter.

Fig. 10. E-Certificate (user interface).

DATA OF CERTIFICATE

欄位	資料
頒發單位	南臺科大區塊鏈技研中心
學校	南台科技大學 資訊工程系
學生	冀謙
出生日期	捌拾伍 年 柒 月 拾捌 日
修業日期	中華民國 壹零參 年 玖 月
英文名字	Chien Chi
頒發日期	中華民國 壹零柒 年 陸 月

Here will show all the certificate data on the certificate.

Fig. 11. Certificate profile.

2) *Users*

ISBN 978-1-5386-4342-6

After the certification unit has issued a certificate, the graduate can look up their certificate by signing into the system (Fig. 12).

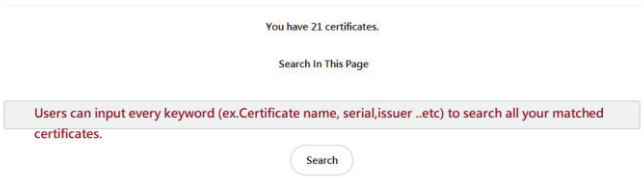

Fig. 12. Inquiry page (for users).

3) *Companies and Employment Agencies*

When a company acquires a serial number or QR code from a job applicant, they sign into the system to verify the veracity of the associated certificate. The message "Valid Certificate" is displayed when the information from applicants matches the information in the blockchain system (Figs. 13–16).

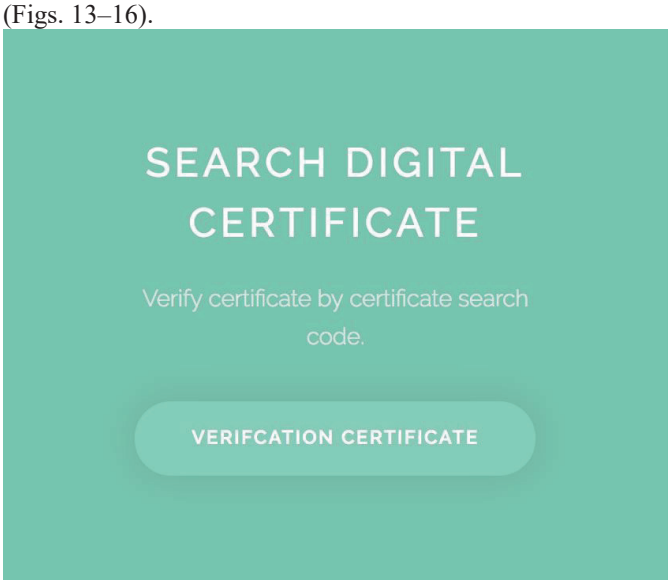

Fig. 13. Inquiry page (for companies).

Fig. 14. Companies inquire about a certificate by entering the serial number sent by the applicant.

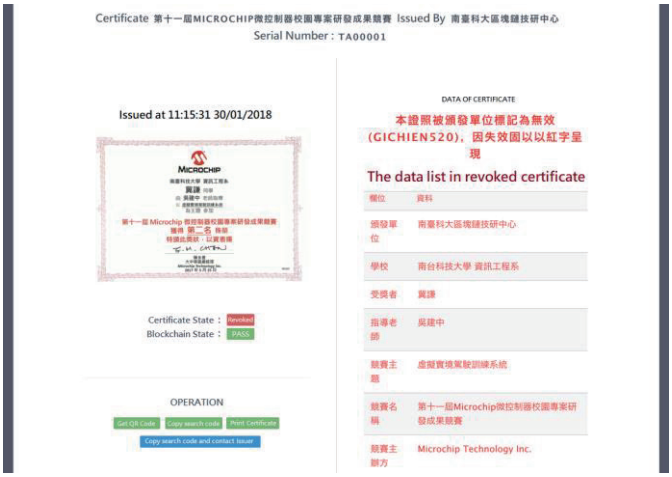

Fig. 15. Certificate verification (the page depicts fail verification).

ISBN 978-1-5386-4342-6

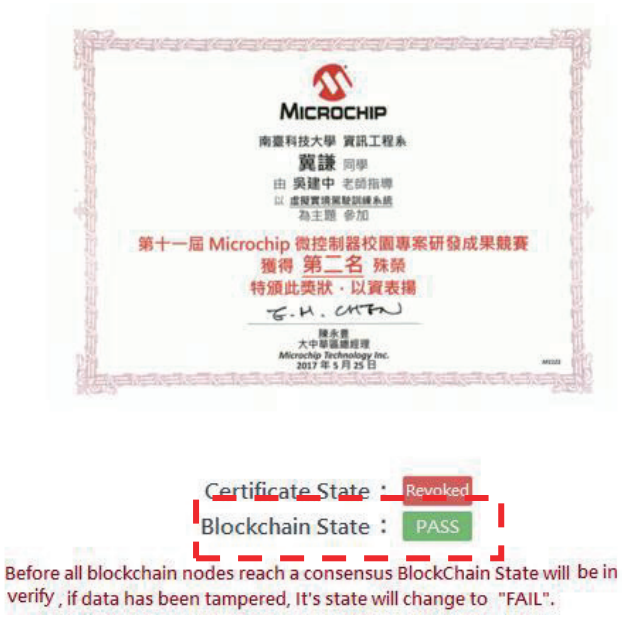

Fig. 16.Blockchaib successful verification.

Conclusion

Data security is one of the major features of blockchain technology. Blockchain is a large and open-access online ledger in which each node saves and verifies the same data. Using the proposed blockchain-based system reduces the likelihood of certificate forgery. The process of certificate application and automated certificate granting are open and transparent in the system. Companies or organizations can thus inquire for information on any certificate from the system. In conclusion, the system assures information accuracy and security.

Acknowledgement

This work was supported by the Ministry of Science and Technology under Project MOST 107-3114-E-492-001.

References

[1] Tengyu Yu, Blockchain operation principle analysis: 5 key technologies, iThome, https://www.ithome.com.tw/news/105374

[2] Jingyuan Gao, The rise of virtual currencies! Bitcoin takes the lead, and the other 4 kinds can't be missed. Digital Age, https://www.bnext.com.tw/article/47456/bitcoin-ether-litecoin-ripple-differences-between-cryptocurrencies

[3] Smart contracts whitepaper, https://github.com/OSE-Lab/learning-blockchain/blob/master/ethereum/smart-contracts.md

[4] Gong Chen, Development and Application of Smart Contracts, https://www.fisc.com.tw/Upload/b0499306-1905-4531-888a-2bc4c1ddb391/TC/9005.pdf

[5] Weiwei He, Exempted from cumbersome auditing and issuance procedures, several national junior diplomas will debut next year.iThome，https://www.ithome.com.tw/news/119252

[6] Xiuping Lin, "Semi-centralized Blockchain Smart Contracts: Centralized Verification and Smart Computing under Chains in the Ethereum Blockchain", Department of Information Engineering, National Taiwan University, Taiwan, R.O.C., 2017.

[7] Yong Shi, "Secure storage service of electronic ballot system based on block chain algorithm", Department of Computer Science, Tsing Hua University, Taiwan, R.O.C., 2017.

[8] Zhenzhi Qiu, "Digital certificate for a painting based on blockchain technology", Department of Information and Finance Management, National Taipei University of Technology, Taiwan, R.O.C., 2017.

[9] Weiwen Yang, Global blockchain development status and trends, http://nmart.pixnet.net/blog/post/65851006-%E5%85%A8%E7%90%83%E5%8D%80%E5%A1%8A%E9%8F%88%E7%99%BC%E5%B1%95%E7%8F%BE%E6%B3%81%E8%88%87%E8%B6%A8%E5%8B%A2

[10] Benyuan He, "An Empirical Study of Online Shopping Using Blockchain Technology", Department of Distribution Management, Takming University of Science and Technology, Taiwan, R.O.C., 2017.

[11] Chris Dannen，Introducing Ethereum and Solidity，https://www.apress.com/br/book/9781484225349

[12] Jan Xie, Serpent GitHub, https://github.com/ethereum/wiki/wiki/%5B%E4%B8%AD%E6%96%87%5D-Serpent%E6%8C%87%E5%8D%97

[13] Solidity ， https://solidity.readthedocs.io/en/latest/index.html

ISBN 978-1-5386-4342-6