Online Certificate Validation Using Blockchain

Shanmuga Priya R,
Department of Computer Science and Engineering, Prathyusha Engineering College,
Thiruvallur,TamilNadu
Swetha N
Department of Computer Science and Engineering, Prathyusha Engineering College,
Thiruvallur,TamilNadu

----------**ABSTRACT**----------

Lakhs of people getting Degrees year after year, 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 block chain technology. All the illegal activities filled against a person and all the activities are updated in the Personal ID. Using the modification process we would monitor not only the degree cortication alone but also entire personality and behavioral activities of that person. We deploy Unique based monitoring using this system.

Keywords – **Block chain, hyperledger, digital certificate, hashing.**

I. INTRODUCTION

1.1 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.

1.2 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.

1.3 Objectives

In this study, we developed a decentralized application and designed a certificate system based on E/thereumblockchain. 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.

II. EXISTING SYSTEM

The certificate are stored in centralized manner and verified manually, so it takes too much time to verify. There is no safety to the certificate that are given to any private sectors (banks).But,thedatas may be changed, deleted or modified. Certificates are easily hacked and make duplicate of that certificate. Students bring their certificates on interview places. There is no security for certificates.

III. LITERATURE REVIEW

3.1 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 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.

The emergence of Ethereum Smart Contracts in 2013 boosted blockchain technology, which became blockchain 2.0. As presented in 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 .

3.2 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:

- 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;
- 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 Ethereumblockchain. This completes the whole process

3.3 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 Ethereumblockchain. 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. 1. Uses of smart contracts.

IV. MODULES

4.1 User Interfaces

User interface design which we use to this project is netbeans and android studio. For server communication we develop an IDE using Netbeans. Using android studio we develop an android application to share and scan the QR code. Testrpc is a Node.js based Ethereum client for testing and development. It uses ethereumjs to simulate full client behavior and make developing Ethereum applications much faster. It also includes all popular RPC functions and features (like events) and can be run deterministically to make development a breeze.

4.2 Verification

In this module user will upload the certificates like 10 th mark list, plus two mark list , college certificates, government certificates and so on. Before upload ,those certificates will verified by the corresponding sector ,if we upload school certificate, the certificate number will check with corresponds school database server if that certificate is verified after that it will stored on server otherwise it will discard.

4.3 Block Creation

A block is a container data structure. The average size of a block seems to be 1MB (source). Here every certificates number will be created as a block. For every block an hash code will generate for security.

4.4 Android based QR code generation:

In this module, based on certificate numbers QR code will generate. While creating QR code user can increase the count based on their needs. The major advantage of this module user can share the QR code to another person in case of necessity. When user scan the QR code an OTP will be send to the registered mobile for verification. After proper authentication user can view their certificates. If third person scan the QR code beyond the permitted limit, the third person's location will send to the authorized user with permission link.From that link user can allow or deny the person.

V. LITERATURE SURVEY

[1] Jiin-Chiou Cheng, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen(2018) 'Blockchain and Smart Contract for Digital Certificate'

Developed a decentralized application and designed a certificate systembased 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.

[2] Murat Yasin Kubilay, Mehmet SabırKiraz and Hacı Ali Mantar(2018) 'CertLedger: A New PKI Model with Certificate Transparency Based on Blockchain'

The current trust model, CAs have the absolute responsibility to issue correct certificates for the designated subject. However, CAs can still be compromised and fake but valid certificates can be issued due to inadequate security practices or non-compliance with the Certificate Policy(CP) and Certificate Practice Statement(CPS).

[3] Marco Valdi, Franco Chiaraluce, Emanuele Frontoni, Luca Spalazzi(2017) 'Certificate validation through public ledger and blockchain'

The project is proposed for the solution of addressing the issues of reliability and security of certificate revocation information. Its main advantages are in removing any single POF and being relatively simple to implement by leveraging existing open source platforms.

[4] Rujia Li, Yifan Wu(2016) 'Block chain based academic certificate authentication system'

The project consists in designing and implementing by conflating the hash value of local files to the blockchain but remains numerous issues, did an effective technological approach protecting authentic credential certification and reputation appear.

[5] Ze Wang, Jiwu Jing, Daren Zha, JingqiangLin(2016) 'Blockchain based certificate transparency and revocation transparency'

In this they maintain a database to record the certificates and revocation status information in the global certificate blockchain which is inherently append only, to achieve certificate transparency and limited grained revocation transparency.

VI. RESEARCH METHODS

6.1 System Design

In this study, a blockchain certificate system was 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, 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

6.3 Process

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

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. The certificate system verifies all the data.

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.

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

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.

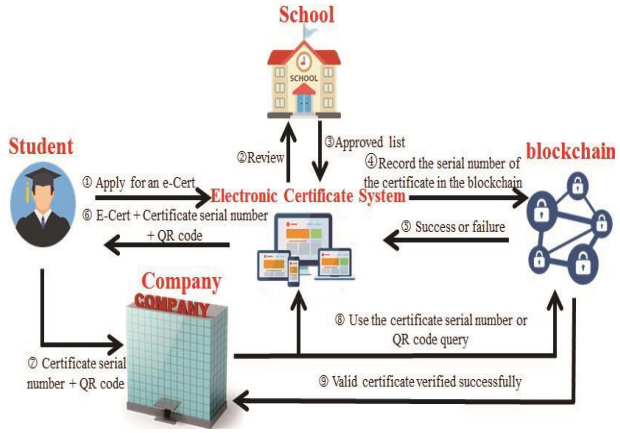

Fig. 2. Working process of the system

6.3 C. Operation

On the sign in page, the user clicks "register now," fills in their basic information, and receives a confirmation email

1) Certification Units

After certificate units 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 inquirynumber to the graduate for future inquires

VII. 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, thesystem assures information accuracy and security.

VIII. 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] JingyuanGao, 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-li tecoin-ripple-differences-between-cryptocurrencies

[3] Smart contractswhitepaper, 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 EthereumBlockchain",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] ZhenzhiQiu, "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://nmarlt.pixnet.net/blog/post/65851006-%E5%85% A8%E7%90%83%E5%8D%80%E5%A1%8A%E9%8 F%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, IntroducingEthereum 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 Solidity , https://solidity.readthedocs.io/en/latest/index.html