CERTIFICATE MANAGEMENT AND VALIDATION SYSTEM USING BLOCKCHAIN

Mili Rafi[1], Sherin Mary Shaji[2], Prof. Ashly Thomas[3]

[1],[2]Graduates, Dept. of Computer Science and Engineering, St. Joseph's College of Engineering and Technology, Palai, Kerala, India.
[3]Assistant Professor, Dept. of Computer Science and Engineering, St. Joseph's College of Engineering and Technology, Palai, Kerala, India.

---***---

Abstract - Every year lakhs of students graduating from different university. The graduation certificates issued by universities and other educational institutions are among the most important documents for graduates. It is an asset for each students. Nowadays everyone has to show his/her Document and Certificate to any other person for some purpose/job. After seeing the document third person cannot validate the originality of the certificate. Verifying a diploma/certificate today takes a good amount of time and requires human resources or human resources to request confirmation of details from universities. The advance of information technology and the availability of low-cost and high-quality office equipment in the market have enabled forgery of important documents such as certificates, identity cards, passports etc. The goal of this paper is to propose a certificate management and validation system that can offer a potential solution for academic certificate issuing and verification using blockchain technology. The blockchain technology contains several functions including hash, public/private key cryptography, digital signatures, peer-to-peer networks and proof of work. The beneficiary or the institution receiving the certificate as a proof of credential would get a clear view on the history of the certificate. The certificate also contains the immutable record of issuing authority, owner of the certificate and date and time of issuance.

***Key Words*: Authenticity, Blockchain, Digital certificate, Hash, Hyperledger.**

1. INTRODUCTION

Universities issue certificates to students who have completed the graduation. A graduation certificate is mostly in the form of a paper-based document, an electronic document cannot effectively replace a physical certificate . However, due to the presence of advanced and cheap scanning and printing technologies, the forgery of certificates has increased. This threatens the integrity of the certificate holder and the university that issued the certificate . It is necessary to validate that the graduation certificate presented by the graduate is genuine and the holder is the rightful owner[5]. Moreover, a graduation certificate has to be verified to ensure that its content is correct and also to ensure that the certificate comes from an authentic source.

To check the validity, much time will be spent in either reaching out to the university to verify a certificate or in awaiting a reply from the university to confirm that the certificate is valid, and the information is accurate. This process can be extremely laborious and expensive. Making certificates easily verifiable is one advantage of digital systems. In our project , we have decided to explore the field of blockchain to implement our solution. The platform used for implementation is Hyperledger.

2. LITERATURE REVIEW

2.1 Blockchain

Blockchain is one of the latest technology, which enables new forms of distributed software architecture. The blockchain data structure is a time-stamped list of blocks, which records and aggregates data about transactions that have ever occurred within the blockchain network. The blockchain provides an immutable data storage, which only allows inserting transactions without updating or deleting any existing transaction on the blockchain to prevent tampering and revision[4]. Each transaction can be separately verified by using its hash value, since it is open, publicly verifiable and the data once entered cannot be altered which help in preventing forgery. In blockchain each block of transactions is linked to the previous block by the hash value of preceding block.

Blockchain technology was first introduced as an underlying technology of cryptocurrency Bitcoin[10]. Bitcoin, an electronic payment system, is launched in order to solve the problem of centralization in current payment systems i.e., banks, financial institutions etc., where a central authority is the only authoritative party who is in charge of processing the electronic payments.

The blockchain technology can be used in many domains, which needs the properties of blockchain like bank, health care, business etc. In here, mainly focus on the certificate management and validation. Different datas 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[7]. The whole process is open to the public, transparent, and secure.

2.2 Digital Signature

Digital signatures are designed to guard against tampering and forgery in digital communications. It refers to the process of encrypting a file that needs to be signed by using an encryption algorithm, and generating a verification ciphertext that can be used to indicate identity information of a person, thereby ensuring the integrity and authenticity of the electronic file[8].

Using the digital signature technology of asymmetric encryption technology, the sender encrypts the electronic document information to be sent by using the private key, and the receiver decrypts the file by using the public key, and then compares the decrypted information with the received original text, if the same Explain that the information received is true and complete, otherwise it indicates that the information has been modified.

When Alice and Bob transmits data to each other, it needs to inform the other party's public key in advance. Alice uses the public key to encrypt the message m and then transmits it to Bob. Bob uses the private key to decrypt the information transmitted by A. The process is shown in Figure 1.

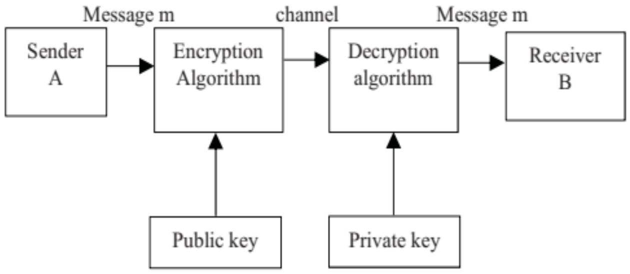

Fig-1: Assymetric Encryption Transcription Process

2.3 Hash

A hash is a shortcode of fixed length. Data input from a document into hash-generator results in a hash output containing a certain number of digits. The hash function is one-way irreversible, and the original input information cannot be calculated from the output, but the input data will have a completely different result as long as it changes slightly. The hash algorithm can effectively verify the integrity of the electronic data. This characteristic of a hash may be used for the detection of any falsification of data and is used in a blockchain mechanism for authentication purposes.

In contrast to digital signatures, hashing is a form of document authentication in which documents are not signed directly. Instead, a hash function generates a hash value to confirm that the authentication of the digital signatures has taken place. There are two components to hashing[6]:

- The hash function is a hexadecimal algorithm, such as SHA-256, that maps an input data of any size into a uniform, usually compressed, file size. In digital preservation, hash functions confirm that no changes have been made to a digital document.
- The hash value is the output of a specific length that permanently identifies the input data.

2.4 Hyperledger

Hyperledger fabric is a distributed ledger technology. The main characteristics of hyperledger fabric is, it is a permissioned network, it supports confidential transactions, to participate one doesn't need cryptocurrency and it is programmable[9]. With these characteristics it establishes trust,Transparency and accountability.

Three main concepts of hyperledger includes asset, chaincode and ledger. Asset is some kind of value which can be exchanged on blockchain system. On hyperledger fabric asset representation be on Json or Binary format. Chaincode defines the structure of asset and also defines the transactions. All transactions are recorded on a ledger. Ledger is a data structure, which tracks all of the asset transactions and it also records state changes of assets.

All blockchain technologies have a concept of nodes, which is a communication entities. All nodes have a valid certificate. There are three types of nodes ; peer (Keeps the ledger data in synch across network),client (initiates the transactions), orderers (responsible for distribution of transactions).

2.4.1 Membership service provider

All entities participate in hyperledger fabric is known and have an identity which is assigned by way of certificates. Members are legally separate entities, these are the organizations that have decided to adopt blockchain for process automation. Each of these members are assigned a certificate and depending on the authority they may be able to use an MSP to create participant and infrastructure component identities within their organization. A blockchain network have more than one Membership service providers (MSP).

2.4.2 Certification Authority

Certification authority (CA) is a trusted third party that affirms the identity of an entity by sighing the certificate containing the entity's public key. There are two other authorities that are referred in the context of CA are the registration authority (RA) and the validation authority (VA)[3]. Fabric CA implementations have two parts: fabric CA server and fabric CA client. Members issue their own identity within their organization. So the hyperledger fabric network can have one or more certification authority to manage the certificates.

2.4.3 Business Network Cards

Business network card contain the configuration information that is needed by the tools and applications for connecting to the business network applications and the hyperledger infrastructure components. There are two administration roles for the BNA; peer admin and network admin. Peer admin creates the network admin and the network admin creates different participants in BNA. The business network card contains the credentials and the composer connection profile. Composer CLI is used for managing the cards.

2.4.4 Fabric Composer

A composer is an open development toolset/framework which makes it easy for creation and management of business network application. The primary goal is to accelerate the development of blockchain applications on hyperledger. The benefits of using hyperledger composer are; it reduces the time to value, it hide the complexity of underlying infrastructure, easy to develop smart contracts and it offers business modeling capability. Many tools are available in the toolset like tools for developers, operations, administrators and business analyst.

3. SYSTEM PROCESS

Hyperledger Fabric will allow only approved participants to read and write on the student certificate. Moreover, blockchain technology ensures that all updations held are accurate and tamper-proof. The three main participants are University/Admin, student and verifier (the student allows to access).

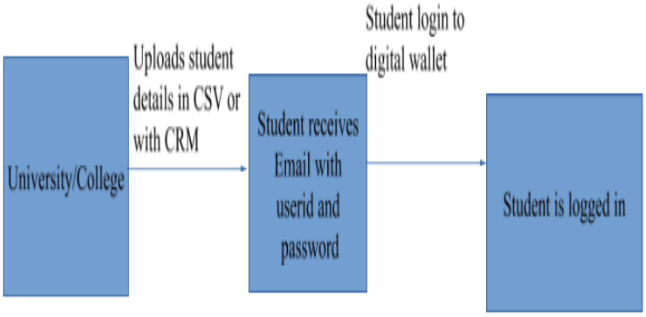
University/College
Uploads student details in CSV or with CRM
Student receives Email with userid and password
Student login to digital wallet
Student is logged in

Fig-2 Diagram of student login

Figure.2 shows process flow of student login. The university or admin uploads the student details . Then the student receives an Email with userid and password. By entering with this userid and password, student can login and view. Only the admin/university can make changes in the certificate and other details.

The details that the admin entered will be moved to the hyperledger fabric. We cannot directly connect to the hyperledger fabric , it will be done via composer Rest Server.

The fig.3 shows the process flow diagram of certificate issuance. When the admin an account, full details of student is getting stored. Then creates a certificate preview, the university verify that and enters the digital signature. Then generates a hash code. The approved certificate is deployed in hyperledger. Students can now receives a copy of certificate using a QR code.

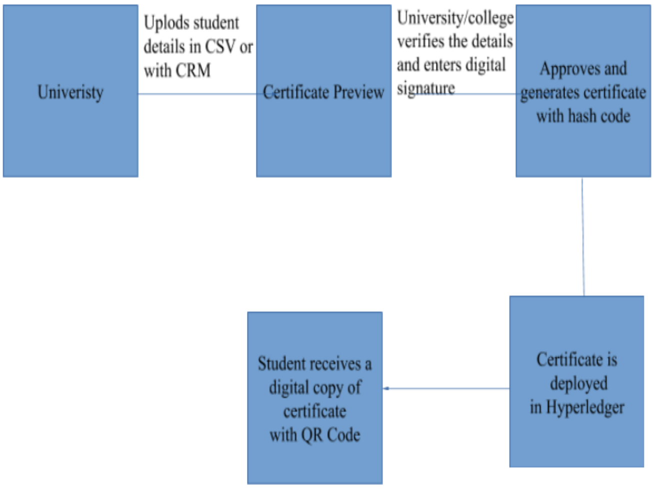
Univeristy
Uplods student details in CSV or with CRM
Certificate Preview
University/college verifies the details and enters digital signature
Approves and generates certificate with hash code
Certificate is deployed in Hyperledger
Student receives a digital copy of certificate with QR Code

Fig-3 Diagram certificate issuance

The certificate is stored in JSON and pdf format. The pdf copy is uploaded to inter planetary file system node and the hash pointer is saved. The JSON file is imported by hyperledger to create an asset. IPFS is a peer-to-peer distributed file system that seek to connect the computing devices with the same system of files.

Third party verifier is one of our participant. By using this system the verifier can easily verify without any difficulties. The verifier receives a QR code from student , using that the verifier can view the certificate. All the history of student mark list is recorded. So without any doubt the verifier can easily understand.Figure 4 shows the diagram of third party verification.

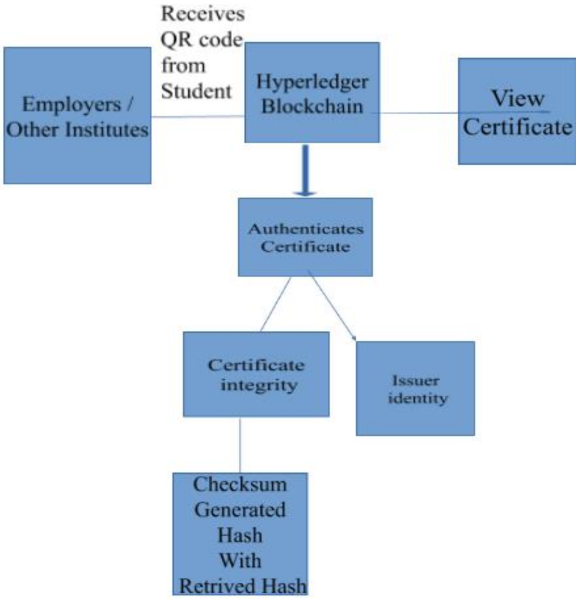
Receives QR code from Student
Employers / Other Institutes
Hyperledger Blockchain
View Certificate
Authenticates Certificate
Certificate integrity
Issuer identity
Checksum Generated Hash With Retrived Hash

Fig-4 Third party verifier

4. CONCLUSION

Using blockchain it is now possible to create a certification infrastructure that puts in record of our accomplishments. This allows us to share our credentials with respective validators. Now a days more researches based on different applications of blockchain are going on. For example in medical field, a healthcare record management system which will definitely useful[2].

REFERENCES

[1] Ruksudaporn Wutthikarn and Yan Guang Hui. “Prototype of Blockchain in Dental care service application based on Hyperledger Composer in Hyperledger Fabric framework”, IEEE, Vol. 4, 2018.

[2] Tagrid Alshalali, Kenneth M’Bale D.Sc and Darsana Josyula Ph.D. “Security and Privacy of Electronic Health Records Sharing Using Hyperledger Fabric”, International Conference on Computational Science and Computational Intelligence (CSCI), vol. 4,2018.

[3] Osman Ghazali and Omar S. Saleh. “A Graduation Certificate Verification Model via Utilization of the Blockchain Technology”, Journal of Telecommunication, Electronic and Computer Engineering., vol. 6,2018.

[4] Jiin-Chiou Cheng, Narn-Yih Lee , Chien Chi , and Yi-Hua Chen. “Blockchain and Smart Contract for Digital Certificate”, IEEE International Conference on Applied System Innovation, Vol. 6, 2018.

[5] S.Sunitha kumari1 and D.Saveetha. “Blockchain and Smart Contract for Digital Document Verification”, International Journal of Engineering & Technology, Vol. 4, 2018.

[6] Nitin Kumavat , Swapnil Mengade , Dishant Desai and JesalVarolia. “Certificate Verification System using Blockchain”, International Journal for Research in Applied Science & Engineering Technology (IJRASET),Vol.7, issue .IV, April 2019.

[7] Yangpeng Zhu,Jiabao He, Kun Yuan and Yanmei Yang. “Research on Modify Protection of Metrology Electronic Certificate Based on Blockchain Technology”,14th International Conference on Computer Science & Education (ICCSE 2019).

[8] Stephen Thompson. “The preservation of digital signatures on the blockchain”, the University of British Columbia iSchool Student Journal, Vol. 3 (2017).

[9] Binh Minh Nguyen, Thanh-Chung Dao and Ba-Lam Do. “Towards a blockchain-based certificate authentication system in Vietnam”, PeerJ Comput. Sci. 6:e266 http://doi.org/10.7717/peerj-cs.266,2020.

[10] Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Giuseppe Gottardi, Daniele Sciarroni and Luca Spalazzi. “Certificate Validation through Public Ledgers and Blockchains”, in Proc. The First Italian Conference on Cybersecurity (ITASEC17), 2017.