RES MILITARIS
REVUE EUROPEENNE D ETUDES EUROPEAN JOURNAL OF MILITARY STUDIES
Social Science Journal

Verification and Validation of Certificate UsingBlockchain

[1]P. Naga Triveni, [2]Dr. G. JawaherlalNehru, [3]Dr. R. Santhoshkumar, [4]S. BavanKumar
[1,4]Assistant Professor, [2,3]Associate Professor
[1]Department of CSE-AIML, [2,3,4]Department of CSE
St. Martins Engineering College , Secunderabad, Telangana

Abstract: According to the Indian Ministry of Education statistics, document verification is a complex domain that involves various challenging and tedious processes to authenticate. Due to the lack of an 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. For students, educational certificates are the most important documents issued by their universities. However, as the issuing process is not that transparent and verifiable, fake certificates can be easily created. A skillful generated fake certificate is always hard to detect and can be treated as the original. With the increase of forged documents, the credibility of both the document holder and the issuing authority is jeopardized. In order to solve the problem of counterfeiting certificates,the digital certificate system based on blockchain technology would be proposed. By the modifiable property of blockchain, the digital certificate with anti-counterfeit and verifiability could be made. The procedure of issuing the digital certificate a 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. In this research, the authors have identified the security themes required for document verification in the blockchain.This research also identifies the gaps and loopholes in the current blockchain-based educational certificate verification. 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.

Index Terms - Blockchain,Smart contract,Digital certificate ,Metamask.

I. Background Information

Maharashtra went through a few vacillations last year as for the retail cost of onions. The cost expanded from Rs. 26 for each kilo in the primary portion of the year to an incredible Rs. 50 for every kilo in August. Noticing the shoot in the value, a considerable lot of the ranchers in the state chose to develop onions on their homestead, in the expectation of making 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 usedfor 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.Blockchain is a distributed database that is widely used for 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 : Rational

A. 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.

II. 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 types are distributed in distinct blocks, enabling verifications to be made without the useof 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 Blockchain.

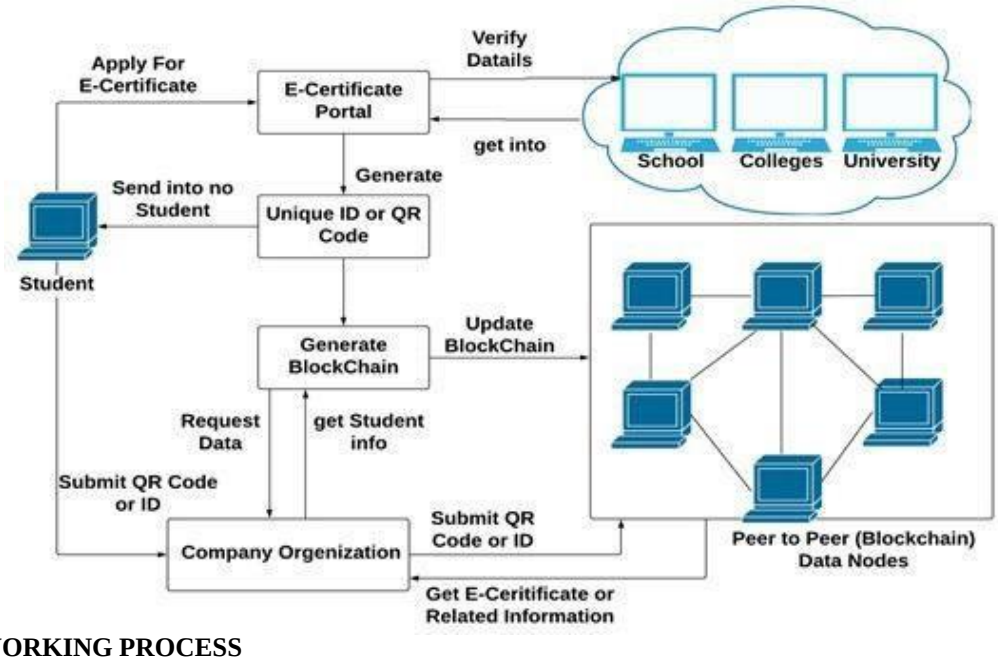
B. History of Blockchain

A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant's ledger. The decentralised database managed by multipleparticipants is known as Distributed Ledger Technology (DLT).Blockchain is a type of DLT in which transactions are recorded with animmutable cryptographic signature called a hash.This means A simple analogy for understanding blockchain technology is a Google Doc. When we create a document and share it with a group of people, the document is distributed instead of copied or transferred. This creates a decentralized distribution chain that gives everyone access to the document at the same time. No one is locked out awaiting changes from another party, while all modifications to the doc are being recorded in real-time, making changes completely transparent

C. Blockchain Hash Function

A hash function takes an input string (numbers, alphabets, media files) of any length and transforms it into a fixed length. The fixed bit length can vary (like 32-bit or 64-bit or 128-bit or 256-bit) depending on the hash function which is being used. The fixed-length output is called a hash. This hash is also the cryptographic byproduct of a hash algorithm. We can understand it from the following diagram.

III. SYSTEM ARCHITECTURE



WORKING PROCESS

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 recordsthe 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. Eachgraduate 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.

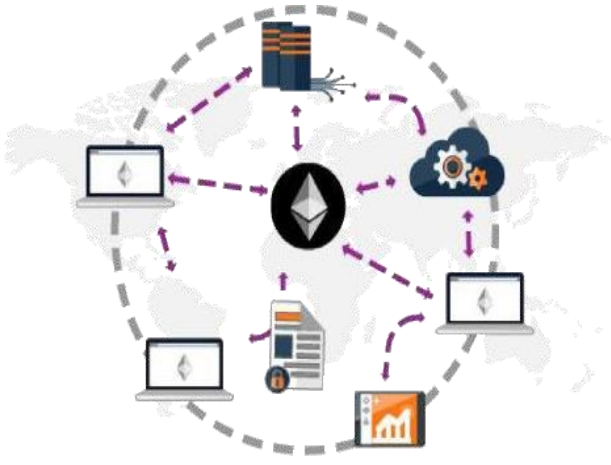
OPRATIONS:

E-certificate generation system which manually creates the certificates based on current students data. Various centralized methods follow the similar approach for verification. The entralized approaches cant defend the various network attacks like SQL injection, Collusion,bruited force etc. Blockchain approach using decentralized approach. Fog computing or fognetworking, also known as fogging, is pushing frontiers of computing applications, data, and services

away from centralized cloud to the logical stream of the network edge. Fog networking system works on to build the control, configuration, and management over the Internet backbone rather than the primarily control by network gateways and switches those which are embedded in the LTE network. We can illuminate the fog computing framework as highly virtualized computing infrastructure which provides hierarchical computing facilities with the help of edge server nodes. These fog nodes organize the wide applications and services to store and process the contents in close proximity of end users.

ETHEREUM:

Ethereum is a **blockchain** platform with its own cryptocurrency,called Ether (ETH) or Ethereum, and its own programming language, called Solidity. As a blockchain network, Ethereum is a decentralized public ledger for verifying and recording transactions. Its cryptocurrency is now second only to Bitcoin in market value.It is the fuel that runs the network. It is used to pay for the computational resources and the transaction fees for any transaction executed on the Ethereum network. Like Bitcoins,ether is a peer-to-peer currency. Apart from being used to pay for transactions, ether is also used to buy gas,
which is used to pay for the computation of any transaction made on the Ethereum network.



IV. PROCESS

Educational documents verification is very tedious and time consuming process in real time environment. E-Certificategeneration for entire educational history is easy process to eliminate such consuming tasks.

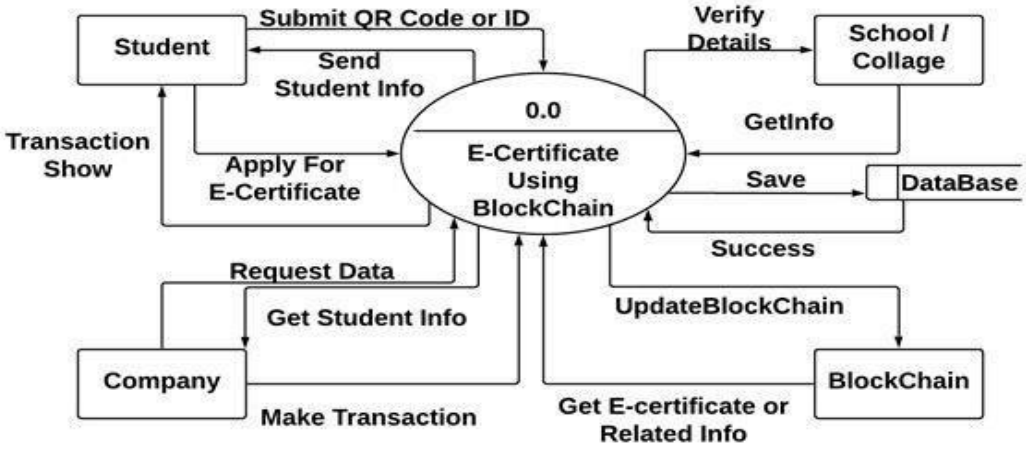
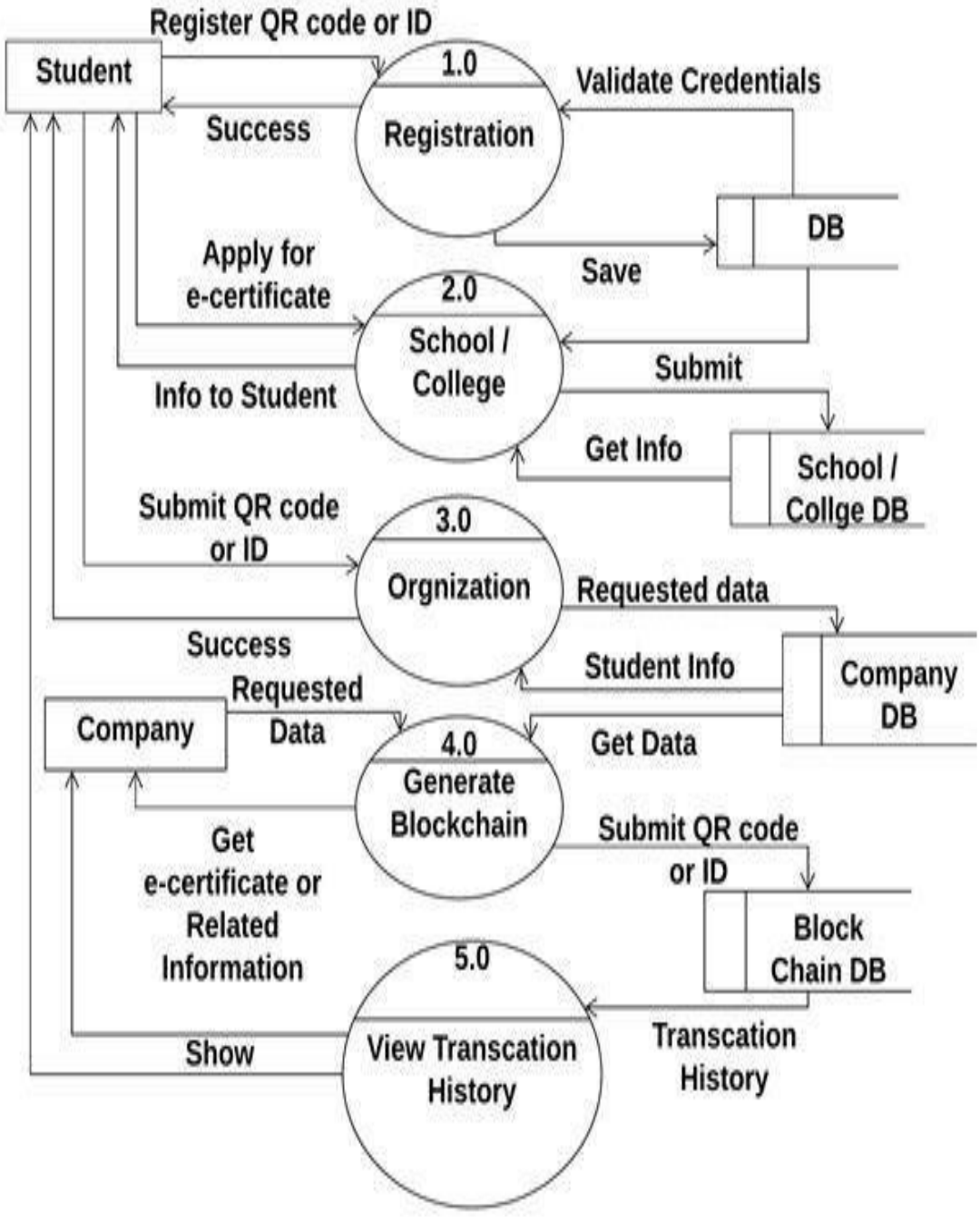


Fig. Process

Dynamic QR-code andunique certificate generation for each students document in proposed system. Data e-certificate stored into the blockchain in secure Manner which enhance the security. According to the smart contract system also allow the updates in entire blockchain.This research proposed a custom blockchain generation on open source platform.


Register QR code or ID
Student
1.0
Registration
Validate Credentials
Success
DB
Save
Apply for
e-certificate
2.0
School /
College
Submit
Info to Student
Get Info
School /
Collge DB
Submit QR code
or ID
3.0
Orgnization
Requested data
Success
Student Info
Company
DB
Company
Requested
Data
4.0
Generate
Blockchain
Get Data
Get
e-certificate or
Related
Information
Submit QR code
or ID
Block
Chain DB
5.0
Show
View Transcation
History
Transcation
History

OUTCOMES:

To create the blockchain based unmodifiable certificates, initially the university needs to get registered.

Any transaction can be sent through the wallet address of the Registered university. Only the owner of the smart contract has the authority to add the universities.Once added the university, will be able to access the system and can create Certificates with data fields. Each created certificate will be stored in the Inter planetary file system (IPFS). It will then return the unique hash generated using SHA-256 algorithm.This will serve as unique identity for each document his generated hash and detail of certifi-cates willbe stored in the blockchain and the student will be provided with the resultant transaction id. Anyone can use this transaction id to verify the certificate details and can view the original copy of certificate using IPFS hash stored along with data. And it is not using the same data. Hence with this we can solve the problem of certificate frogery.

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.

REFERENCE :

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-li tecoin-ripple-differences-between-cryptocurrencies

3] Smart contracts whitepaper, https://github.com/OSE-Lab/learning-blockchain/blob/ master/ethereum/smart-contracts.md4] 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.

6] 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.

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

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

12] Solidity https://solidity.readthedocs.io/en/latest/index.html