Educational Certificate Verification System Using Blockchain

Dinesh Kumar K, Senthil P, Manoj Kumar D.S

Abstract: Academic certificate verification is routine process for the employer for offering employment. Employer takes much time for giving offer letter after the interview process gets over. To verify the originality of the certificate the employer need to authenticate the certificate from the certificate issuing authority. The employer takes much time for certificate verification to check the originality of the certificate. The overall certificate verification process takes longer time to complete the selection process. In order to solve this problem, Blockchain provides verifiable distributed ledger with cryptography mechanism to counterfeit academic certificate. The Blockchain also provide a common sharing platform for storing, accessing document and minimize the overall time for verification.

Index Terms: Blockchain, Digital Certificate, Distributed Ledger, Hashing, Ethereum, Cryptography, Counterfeit

1 INTRODUCTION

The Blockchain concept was proposed as bitcoin by Satoshi Nakamoto in early 2008 [1]. Blockchain is a distributed ledger which provides decentralized and data sharing. Each Block contains set of transaction, these transaction could be cryptocurrency transaction, digital certificate, bill of lading etc., the transaction data should replicated to all the nodes to form identical transaction details in ledger. The transaction details are validated by intermediators, there after the valid transactions are updated and new mined block will appended with longest chain [1]. Blockchain transaction are cryptographically sealed which ensure security.

2 RELATED WORK

2.1 Blockchain

Blockchain is a system that does not rely on the trust for electronic transaction. It shows how the problem of double spending can end Resolve the history of each transaction using a peer-to-peer network to record the history of each transaction later It is computationally impossible to transfer to the intruder if the legitimate ends of the system control the majority of CPU power. Nodes can join or exit the network whenever needed. They vote with their CPU power, and when the majority is achieved, the module is considered a valid block included in the current long chain and the invalid blocks are not appended with blockchain. It has the characteristic of decentral0ized and temper resistant verification such that it has numerous applications such as Decentralized cryptocurrencies, cross border payments, Blockchain Internet of things (IoT), supply chain management and everledger etc., [2].

The Educational certificates issued by educational institutions are important documents for students and graduates. Proof of Education Certificate and eligible to apply for higher studies and employment. Advances in information technology and the availability of low-cost and high-cost equipment enable fraudulent access to important documents such as identity cards, certificates and passports. Traditional document verification is expensive and the time consuming process of human intervention can lead to academic credential fraud [5]. The trends in information technology in recent years become solution for all the problems such as data protection, consistency and reliability are more important than ever. The job aspirant requires educational certificates to be verified during interviews and higher studies. In some situation, employer can take longer time to verify the originality of certificate, during these verification, candidates has to wait for more number of days to get the offer letter, over all it consumes the time of job aspirants. In this paper the goal is to propose a potential solution for academic certificate issuing and verification using block chain technology [6].

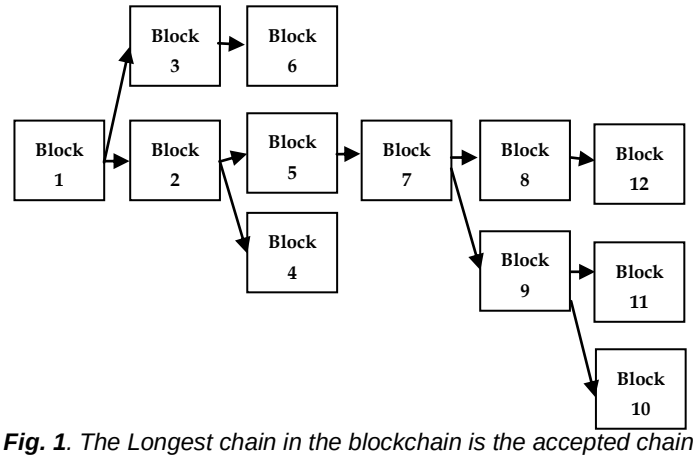

***Fig. 1**. The Longest chain in the blockchain is the accepted chain*

Blockchain is a distributed ledger is used for storing distinct transaction. Each transaction is validated by different nodes. Accepting legal transaction is finalized using consensus algorithm like permission less consensus algorithm and permissioned consensus algorithm. Blockchain are available in two forms the first is Blockchain 1.0 version used for applications such as cryptocurrency, public ledger to main data in replicated form. Blockchain 2.0 is used for decentralized manner which transform assets through smart contract, thereafter automation of transaction is possible.

- *Dinesh Kumar K, Assistant Professor, Department of Information Technology, AMET Deemed to be University, Chennai, Tamil Nadu, India, dineshkumar01@gmail.com*
- *Senthil P, Assistant Professor, Department of Information Technology,*
- *Gojan School of Business and Technology, Chennai, Tamil Nadu, India, pv.senthil25@gmail.com*
- *Manoj Kumar D.S, Assistant Professor, B.S Abdur Rahman Crescent Institute of Science and Technology, Chennai, Tamil Nadu, India, manojkumards03@gmail.com*

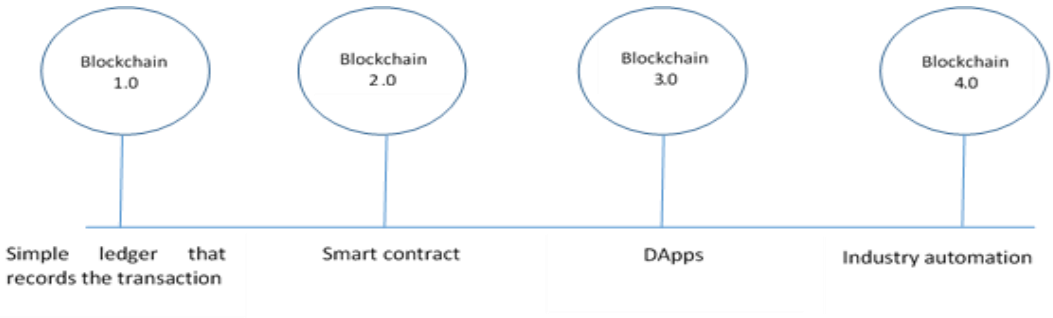

***Fig. 2**. Evolution of Blockchain*

The main aim of Blockchain 1.0, allowing any parties to transact each other directly in untrusted environment. The committed transaction are impossible to reverse the transaction this would help the parties secure from fraud, inconsistency in transaction, ensure same transaction details in ledger to all the parties. Each block in blockchain are cryptographically sealed, the transaction details of current block and block header is hashed using double SHA256 algorithm. The Block header contains previous block hash, time stamp, version, nonce, merkle root hash.

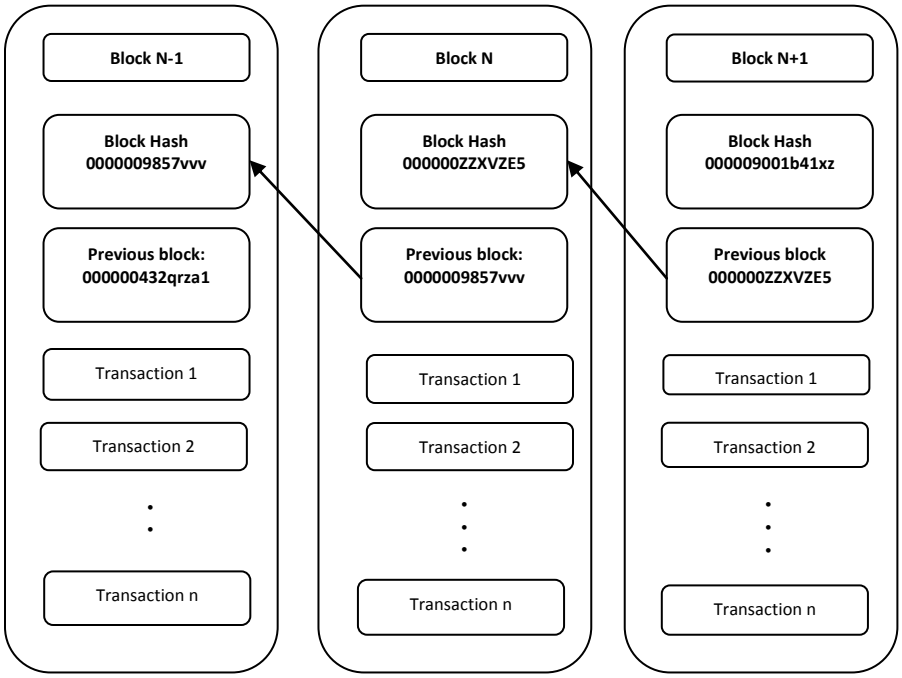

***Fig. 3.** Cryptographically sealed blocks*

2.2.1. Private smart contract

Permissioned blockchain are becoming emerging trends in business collaboration can highly efficiency in closed network. Private blockchain very limited number stakeholder to make business transaction. In public blockchain the validation cost is very expensive. Energy spent on consensus mechanism to perform proof of work is very high when compare to permissioned blockchain. Therefore private blockchain can be efficient if there is limited number of nodes, the transaction speed is good. Consensus mechanism used in private and public blockchain will differ. In public blockchain the consensus algorithm used are Proof of work, Proof of Stake. In private blockchain depends on business requirement the following consensus algorithm is used PAXOS, RAFT, BFT, PBFT, RBFT. To create a blockchain environment for business application IBM provides environment to develop blockchain for business service they are Hyperledger fabrics, Hyperledger composer, Hyperledger Indy and Hyperledger SideDB [3]. Hyperledger Fabric is a permissioned blockchain netwoks that take part in developing the Hyperledger Fabric are called members. The member organization in the network is responsible to assign peers for participating in the network. Every peers in the network get certified by the certificate authority.

2.2.2 Public smart contract

Permissionless blockchain has no requirement for peer nodes to participate, therefore all peer nodes have the authorized to install smarts contracts. To prevent spamming, instantiating and executing smart contracts on a public blockchain, the members required to pay some nominal fee. The smart contracts in public blockchain applications such bitcoin is developed using bitcoin scripts which is used for making contractual terms. Ethereum also can be used in many applications which control money and build many ecentralized application. Eth is also a cryptocurrency developed in Ethereum environment.

2.2.3 Ethererum

Ethereum can be implemented in both private and public blockchain. The first blockchain hold the smart contract to execute business logic. Most smart contracts and decentralized autonomous organizations are created by using Ethereum .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) [7].It provides an infrastructure that enables developers to create applications. The infrastructure is developed and maintained by both Ethereum and those developers [4].

2.2.4 Hyperledger

Hyperledger project is a product of linux foundation. Hyperledger project later transformed to Hyperledger fabric, it is an open distributed ledger for business solutions. Hyperledger fabric which makes private blockchain in closed network. Hyperledger Composer provides solution for business service developed by Business architect. The sideDB is a no sql database used for storing intermediate data.

3. Proposed Work

The students achievements available in the form of degree certificate, mark sheet, value added certificate, etc., will become an important weightage for recruitment or higher studies. The Education institution awards and degree certificates may have only the names of the institution and the student's data. In this scenario there is a lack of effective anti-forge mechanism, due to this events many times the graduation certificate to be forged often is found. To solve the problem of fake certificates, the blockchain technology would stores the certificate in digital form. The immutability nature of blockchain makes digital certificate in the distributed ledger is very difficult to tamper or modify also it is very easy to verify the originality of digital certificate.

3.1 Process

The process of issuing digital certificates in the system is as follows. First step, generate the hash value for certificate using double SHA256. Store the fixed length hash value as a transaction in the block. This transaction is validated by the members in the blockchain, once it is trusted as valid transaction then the block is added with existing blockchain. Accepting and rejecting will be done using consensus algorithm [8]. The consensus algorithm may be chosen based on number of nodes, and transactions. The system will generate the related QR code and inquiry string code to affix in the hardcopy certificate [11]. The system provides the unit to authenticate the hardcopy certificate through phone scanner or website [9]. The immutability nature of the distributed ledger, the system provides not only verification of certificate and also it stores the certificate in digital form forever [10].

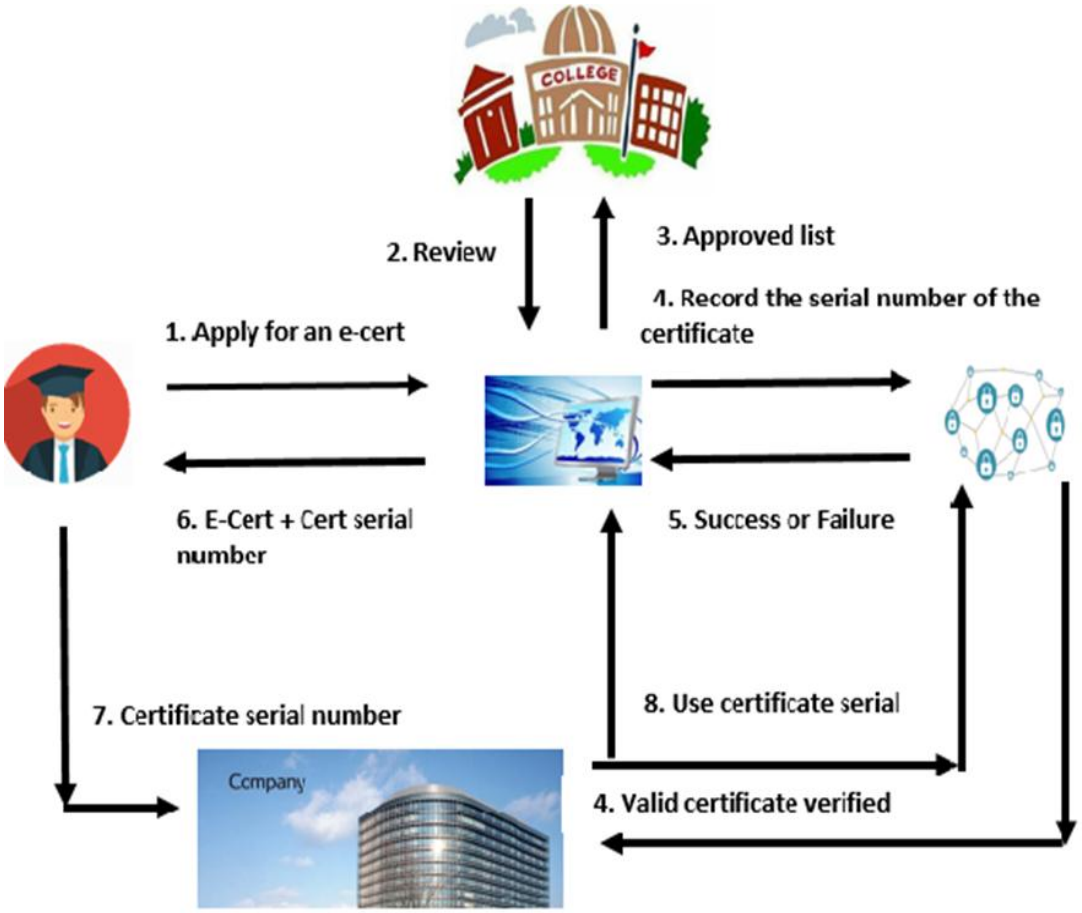

Fig. 4. System Process

4. CONCLUSION

Transparency and data immutability is the main features of blockchain application. It is a distributed ledger where node in the network validate and make final consensus to add the data in the network. The process of academic certificate generation is open and distributed among the parties where any an organization or parties can verify information of any academic certificate using this blockchain system. The Ethereum blockchain also ensures data stored on blockchain network is encrypted, therefore only the certificate owner can see and share this data as they wish. In conclusion, academic institutions are able to collaborate with other employers and publish credentials on the blockchain to eradicate fake educational certificate.

REFERENCES

[1]. S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008; bitcoin.org/bitcoin.pdf.
[2]. “Hyperledger project,” [online] Available: https://www.hyperledger.org/ [Accessed on 5.07.2019]
[3]. IBM Blockchain based on Hyperledger Fabric from the Linux Foundation. Available from https://www.ibm.com/blockchain/hyperledger.html.
[4]. Nachiappan Michael Crosby, Pradan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman, "BlockChain Technology: Beyond Bitcoin", Applied Innovation Review, no. 2, Jun. 2016.
[5]. Tarek Kanan, Ahamd Turki Obaidat, Majduleen Al-Lahham, "SmartCert BlockChain Imperative for Educational Certificates", Electrical Engineering and Information Technology (JEEIT) 2019 IEEE Jordan International Joint Conference on, pp. 629-633, 2019.
[6]. Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Guiseppe Gottardi, “Certificate Validation through Public Ledgers and Blockchains,”In Proceedings of the First Italian Conference on Cybersecurity (ITASEC17), Venice, Italy.
[7]. Jiin-Chiou, Nam-Yih Lee, Chien Chi, YI-Hua Chen, “Blockchain and Smart Contract for Digital Certificate,”Proceedings of IEEE International Conference on Applied System Innovation 2017.
[8]. 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.
[9]. [online] Available: https://www.blockcerts.org.
[10]. Dinesh Kumar K, Komathy K, Manoj Kumar D.S , “Blockchain Technologies in financial sectors and industries”, International Journal of Scientific and Technology Research Volume 8, Issue 11, pp. 942 -946, 2019.
[11]. 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.
[12]. Karuppanan Komathy. (2018). Verifiable and Authentic Distributed Blockchain Shipping Framework for Smart Connected Ships. Journal of Computational and Theoretical Nanoscience. 15. 3275-3281. 10.1166/jctn.2018.7610.