



Academic Credential Attestation using Block Chain Technology

Indu Bala¹ and Pooja Sinsinwar²

¹M. Comm (Business Administration), Maharaja Ganga Singh University, Bikaner

²M. Comm (Business Administration), Rajasthan University, Jaipur

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.

Key words: Blockchain, Digital Certificate, Distributed Ledger, Hashing, Ethereum, Cryptography, Counterfeit

1. INTRODUCTION

The Blockchain concept was introduced in early 2008 by Satoshi Nakamoto as a bit coin. Blockchain is a distributed ledger that provides decentralized and data sharing. Each block contains a set of transactions, be it a crypto currency transaction, a digital certificate, a bill of lading, etc. The transaction data should be copied to all the nodes so that the details of the same transaction are created in the ledger. The details of the transaction are verified by the seller, then when the correct transaction is updated and the new mined block is joined by a long chain the blockchain transaction is sealed with encryption. Has been done to ensure security.

2. RELATED WORKS

Blockchain is a system that does not rely on trust for electronic transactions. It shows how the problem of double spending can be eliminated. Solve the history of each transaction using a peer-to-peer network to record the date of each transaction later. If the legitimate end of the system is controlled, it is impossible for the computation to move the intruder. The majority of CPUs can join or exit the nodes network whenever needed. They vote with the power of their CPU, and when a majority is obtained, the module is considered a valid block in the existing long chain and invalid blocks are not included with the blockchain. It features decentralized and temperament resistance verification that has a wide range of applications such as decentralized crypto currencies, cross-border payments, blockchain Internet of Things (IoT), supply chain management and evolution.

Educational certificates issued by educational institutions are important documents for students and graduates. Proof of education certificate and eligibility to apply for higher education and employment. Advances in information technology and the availability of low-cost and high-cost goods make fake access to important documents such as identity cards, certificates and passports possible. Verification of traditional documents is costly and the time-consuming process of human intervention can lead to academic fraud. In recent years, information technology trends have become the solution to all problems, such as data security, consistency and reliability are more important than ever. Job seekers are required to have an interview and a certificate of education during higher education. In some cases, the employer may take longer to verify the authenticity of the certificate. During these verifications, candidates have to wait for more days for the offer letter, more so it uses the time of job seekers. - the aim of this article is to offer possible solutions for issuing and validating educational certificates using blockchain technology.

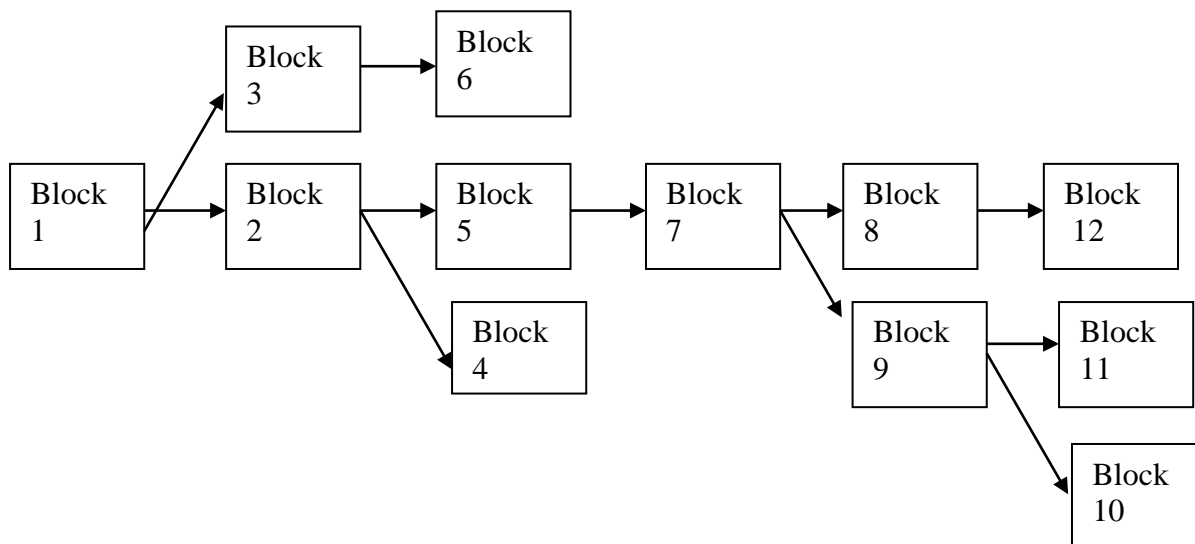


Fig. 1 The Longest Chain in the Blockchain is the Accepted Chain

A blockchain is a distributed ledger used to store individual transactions. Each transaction is authenticated through different nodes. The acceptance of legal transactions is finalized using consensus algorithms such as the Permitted Consensus Algorithm and the Permitted Consensus Algorithm. Blockchain is available in two formats, the first of which is Blockchain version 1.0 which is used for applications such as crypto currency, public ledger in the form of copying important data. Blockchain 2.0 is used for decentralized mode that converts assets through smart contracts, after which automation of transactions is possible.

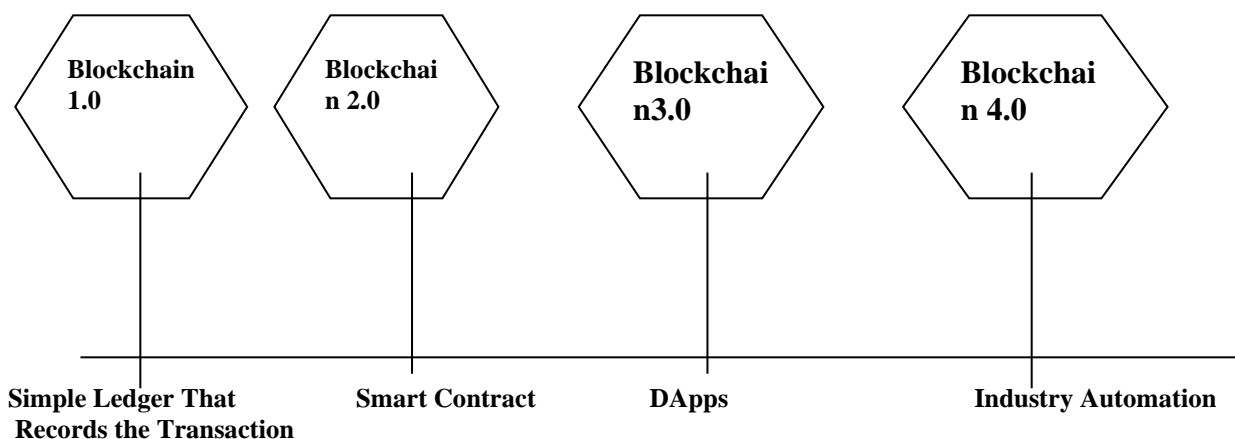


Fig. 2 Evolution of Blockchain

The main purpose of Blockchain 1.0 is to allow any party to transact directly with each other in a trusting environment. It is impossible to divert the transaction from the associated transaction which will help the parties to be safe from fraud, contradiction in the transaction, the details of the transaction will be ensured. In the ledger of all parties. Each block in the blockchain is sealed secretly, the current block and block header transaction details are hashed using the double SHA256 algorithm. Block header includes previous block hash, time stamp, version, nonce, Merkel root hash.

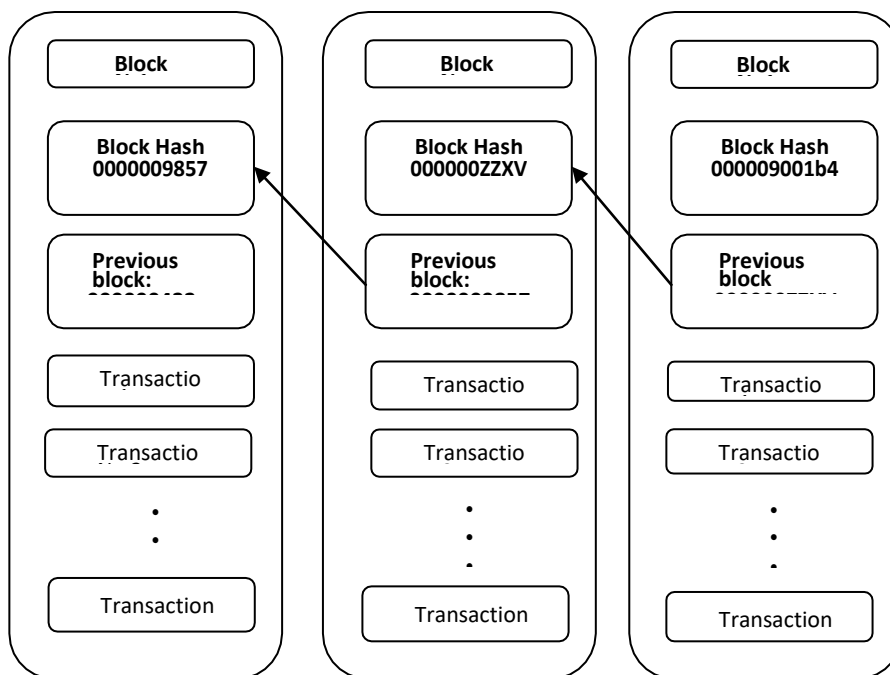


Fig. 3 Cryptographically Sealed Blocks

Private Smart Contract

Emerging trends in business collaboration are emerging in the permitted blockchain closed network. Private Blockchain has a very limited number of stakeholders for doing business. The cost of verification in public blockchain is very expensive. The energy spent on the consensus method to present proof of work is too much when comparing the permitted blockchain. So a private blockchain can be efficient if there are a limited number of nodes, the transaction speed is good. It will be different from the consensus method used in private and public blockchain. The public blockchain uses a consensus algorithm, proof of work, and proof of stack. The following agreed algorithms PAXOS, RAFT, BFT, PBFT, RBFT are used depending on the business needs in the private blockchain. To create blockchain environments for business applications IBM Environmental Business Services provides the environment to create blockchain environments: Hyper Ledger Clothing, Hyper Ledger Composer, Hyper Ledger Hyper ledger indy and hyper ledger side DB. Hyperledger Fabric is an authorized blockchain network that Participate in the manufacture of hyperledger fabric called member. The member organization in the network is responsible for assigning partners to participate in the network. Every peer in the network is certified by a certificate authority.

Public Smart Contract

Peerless Blockchain has no need to participate in Peer Nodes, so all Peer Nodes have the option to install smart contracts. To avoid spamming, instituting and enforcing smart contracts on public blockchain, members are required to pay a small fee. In public blockchain applications, smart contracts such as bit coins are created using bit coin scripts that are used to create contract terms. Ethereum can also be used in many applications that control money and build many sanitary applications. Ethereum is also a crypto currency developed in the environment.

Ethereum

Ethereum can be applied in both private and public blockchain. The first blockchain smart contract to implement business logic. Most smart contracts and decentralized autonomous organizations are created using Ethereum. If bit coin blockchain are considered a global payment network, Ethereum would be a global computing system. Furthermore, Ethereum is an open source platform similar to Android (developed by Google). It provides a basic infrastructure that enables developers to build applications. The infrastructure has been developed and maintained by both Ethereum and the developers.

Hyper ledger

The Hyper Ledger Project is a product of the Linux Foundation. The Hyper Ledger project later evolved into the Hyper Ledger fabric, an open distributed ledger for business solutions. Hyper ledger fabric that creates a private blockchain in a closed network. Hyper Ledger Composer provides a business services solution developed by Business Architect. SideDB is a sql database used to store intermediate data.

3. PROPOSED WORK

Achievements in the form of student degree certificates, mark sheets, value added certificates, etc., will prove to be an important weight for recruitment or higher education. Educational Institution Awards and Degrees Certificates can only contain the name of the institution and student data. In this scenario, there is a lack of effective anti-forgery procedures, which often lead to fake graduation certificates. To address the issue of forged certificates, blockchain technology will store certificates in digital format. The immovable nature of blockchain it is very difficult to tamper with or edit a digital certificate in a distributed ledger, and it is very easy to verify the authenticity of a digital certificate.

Process

The process of issuing digital certificates in the system is as follows. First step, create a hash value for the certificate using double SHA256. Store the default length hash value as a transaction in the block. This transaction is authenticated by the members in the blockchain, once it is trusted as a trusted transaction, and then the block is linked to the existing blockchain. Consent will be accepted and rejected using the algorithm. The consensus algorithm can be selected based on the number of nodes and transactions. The system will generate relevant QR codes and inquiry string codes to affix to hard copy certificates. This system provides the unit with a phone scanner or website to verify the hardcopy certificate. The immovable nature of the distributed ledger, the system not only provides certification and it saves the certificate in digital form forever.

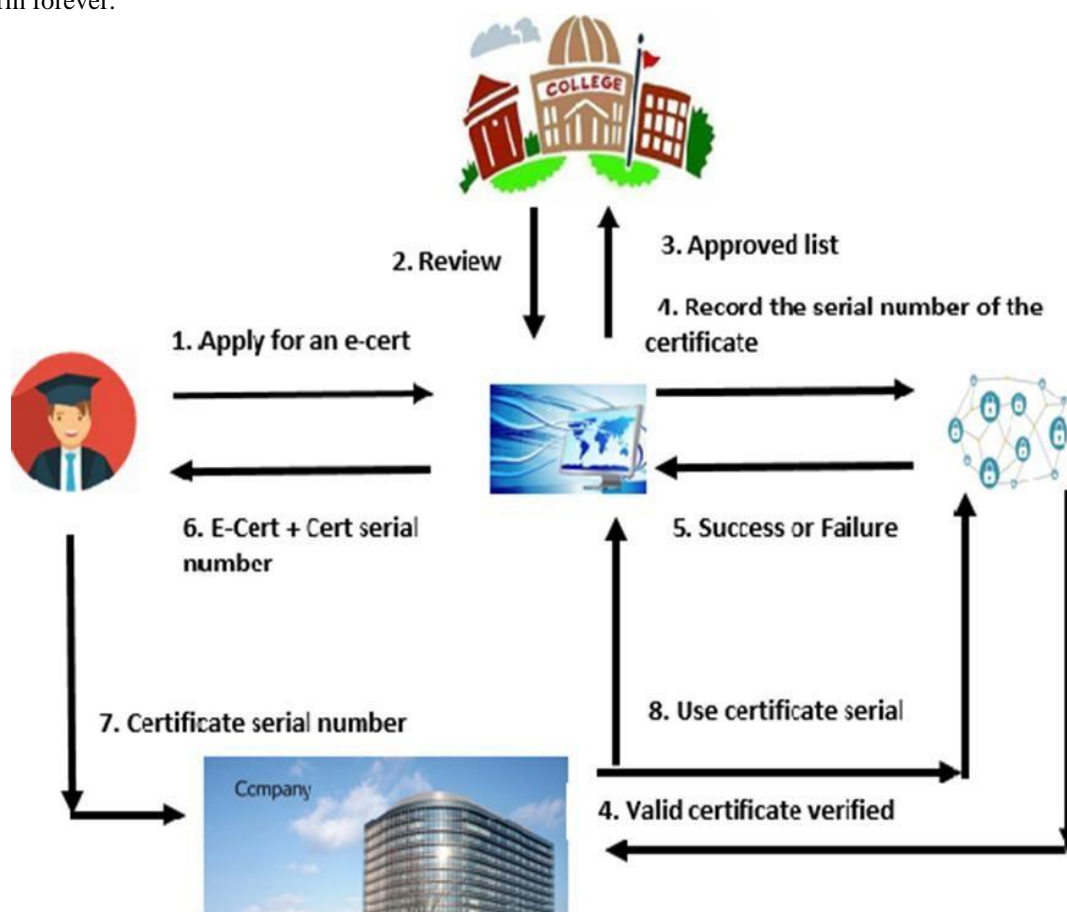


Fig. 4 System Process

4. CONCLUSION

Transparency and data transformation are key features of blockchain application. It is a distributed ledger where the node in the network confirms and finalizes the inclusion of data in the network. The process of generating educational certificates is open and distributed among the parties where any organization or parties can verify the information of any educational certificate using this blockchain system. Ethereum Blockchain also ensures that the data on the blockchain network is encrypted, so only the certificate holder can view this data and share it as they wish. Finally, educational institutions are eligible to collaborate with other employers and publish certificates on blockchain to eliminate fake educational certificates.

REFERENCES

- [1]. S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008; bitcoin.org/bitcoin.pdf.
- [2]. "Hyper ledger project," [online] Available: <https://www.hyperledger.org/> [Accessed on 5.07.2019]
- [3]. IBM Blockchain based on Hyper ledger 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 Bit coin", 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, Guiseppa Gottardi, "Certificate Validation through Public Ledgers and Blockchains," In Proceedings of the First Italian Conference on Cyber security (ITASEC17), Venice, Italy.
- [7]. Jiin-Chiou, Narn-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.