Decentralized Management Solution for Certificate Verification Using Blockchain Technology and Smart Contracts

Priyanka Amol Kadam[1*], Dr. Shashi Bhushan[1], Dr. Sandeep Kadam[2]
[1]*Department of Computer Engineering, Shri. Jagadishprasad Jhabarmal Tibrewala University, Jhunjhunu, India*
[2]*Department of Computer Engineering, B.S.COER, Narhe, Pune, India*

***Corresponding Author:** priyamahadik2007@gmail.com

Abstract:
Today's digital world virtually exclusively uses online processes to initiate and complete transactions. With the development of new technologies, tasks that seemed difficult to complete have become incredibly simple to complete with a minimum amount of error and a maximum amount of reliability. In the field of education, it has been noted that keeping track of and confirming the numerous credentials needed for either job-related or educational admittance purposes is quite challenging. Additionally, it takes more time, and there are several opportunities for the original data to be manipulated. This article puts forth a decentralised certificate management system based on block chain technology and smart contracts. The proposed system serves as a complete and workable solution for the preservation and verification of documents, certificates, and other connected, similar activities without involving any other parties. Through the use of procedure, the framework makes sure that the confidentiality and security of records are preserved. It may also be viewed as a cost-effective option. The Framework that is being presented is a sophisticated use of blockchain technology. It offers a practical and efficient method for issuing, keeping track of, and confirming certificates and other official documents.In this research Hyperledger Fabric technology along with blockchain is used to overcome the problem of certificate verification. Additionally, using smart cards decentralises the essential certification services, increasing data or document dependability, correctness, and privacy. Its uability has tremendous impact on time latency and expenses on the whole process as match up to to the conventional way.

Keywords: Blockchain, Smart contract, Verification, Hyperledger.

1. INTRODUCTION

In today's technologically dominated society, reliable document verification is one of the biggest issues. According to the current situation, certificates are very important when applying for admission to some universities, colleges, high schools, and other educational institutions. On the other hand, they are also important when applying for government jobs, government scholarships, and other government-related benefits. Maintaining, issuing, and validating the numerous documents that the applicants have submitted will present several difficulties. The most difficult issue to solve is how to reliably and securely verify documents without tampering with or changing the original data.So the objective of research is to propose a system which satisfies all the requirnments of verification and validation of the certificates by using Hyperledger Fabric and smart contract.

The framework of decentralized management solution of certificates using blockchain technology and smart contracts is the most dependable and tamper-proof solution to avoid forgery, time latency caused by centralized system, bribers as well as corruption, etc. problems and improves the performance of working framework using advanced technologies. Although email services and cloud computing have the potential to solve many major issues, there are still concerns about security and centralization. Data vulnerability to theft, misuse, or destruction becomes a risk as centralized services for data storage and management are introduced. Due to its decentralization, immutability, scalability,

lack of trust, and privacy control capabilities, blockchain technology is posing as a possible solution to the same problem of data sharing and maintenance. The popularity of the crypto currency among all other technologies is a result of its implementation in a variety of frameworks and applications in the modern world. For instance, the data sharing systems of blockchain technology are widely utilized in e-governments, healthcare facilities, admission-related tasks in various schools, colleges, and universities, in IOT frameworks, and in a variety of other applications in the educational space.

2. LITERATURE REVIEW

Many authors and researchers had come with the ideas that had been developed till date to achieve the Motto of certificate verification which have resolved the problem of forgery with implementing the distributed ledger format for storing the educational records here blockchain infrastructure provides a technical interface for interaction between the procedures in to the management.

Table 1 Author wise review of technology used

AUTHOR	YEAR	RESEARCH WORK	USED PLATFORM	ACCESS	USE OF SMART CONTRACT
SHAIPLES	2019	Educational Records & Online tutor	Ethereum	Private	Yes
BLOCKCERT	2019	Issuing and verifying certificates	Ethereum	Public	No
UNIC	2019	Issuing and verifying certificates	Bitcoin	Private	No
GRNET	2019	Verifying certificates	Cardano	Private	No
TURKANOVIC	2020	Credits Transfer	Ethereum	Public	No
UNICHAIN	2020	Governing transactions & controlling access to academic records	Ethereum	Private	Yes
BOLL	2020	Managing Learning logs	Ethereum	Public	Yes
GUO	2020	Digital rights management for multimedia resources of online education	Ethereum	Public	Yes
BORE	2020	Managing school records	Hyperledger	Private	Yes
RAJU	2021	Identity Manegment	Ethereum	Private	Yes
GAZALI	2021	Managing study loan repayment	Ethereum	Public	Yes

3. RESEARCH METHODOLOGY

Blockchain Technology

In contrast to traditional databases used to store information, blockchain offers a shared database. In a blockchain technology system, information packets or pieces are stored in blocks and connected together via encryption. Information is electronically stored in digital format in blockchain databases.

The technological function of blockchains in cryptocurrency systems, such Bitcoin, Ethereum, and others, for safeguarding transaction records on decentralized platforms, is what makes them most well-known. The revolutionary aspect of a blockchain is that it fosters confidence without relying on third parties by ensuring the security and validity of data records or ledgers.When Satoshi Nakamoto first published the Bitcoin whitepaper in 2008, Safa Nakamoto was the person who gave blockchain technology its biggest boost. an electronic cash system that is peer-to-peer. This invention has improved a number of industries, including manufacturing, finance, healthcare, and education during the past ten years, making it one of the most effective technologies ever created. Information becomes immutable once it is committed to the blockchain. Thus, blockchain can be described as a system that provides a distributed, immutable, secure, and decentralized storage platform. The key components of a blockchain are as follows: Data on a blockchain is logically organized in a series of blocks.

1. Decentralization - With blockchain technology, trust is spread among several nodes and is not dependent on a single entry.

2. Immutability - Data that have been accepted and added to the blockchain are permanently and immutably kept.

3. Consensus - Consensus is the process of a sufficient number of block chain participants deciding on the legitimacy of transactions.

4. Scalability - A block chain system is said to be scalable if it can process more transactions per second than other systems already in use by altering the consensus processes and/or the number of data blocks.

5. Data validity and security - Using consensus and immutability together, blockchain networks can validate and secure data.

6. Privacy Control - The type of blockchain will determine privacy. Data can be restricted to a subset of block chain participants or made available to all participants.

The three types of block chains must be taken into account in accordance with the application requirements in order to construct a block chain-based application. –

Public

There is no one owner and no centralised control over a public blockchain, which is completely decentralised and permissionless. Anyone who wants to engage is welcome in the consensus process. Bitcoin is a prime illustration of a public blockchain.

Private

Private blockchains are those that are owned by a single entity that regulates access to the network of transactions. Consequently, a permissioned blockchain is another name for it. Block creation in this kind of blockchain does not require the use of a consensus algorithm.

Hybrid (consortium)

This blockchain is both permission and public, meaning it is only open to a select number of users. Hybrid blockchain is widly used because of its nature. Also the advantages of both public and private combined. Hence it is most used blockchain in application except the application which are totally public in nature they not refer this hybrid blockchain. Likewise fully Private type application is not referring this type of blockchain.

Hyperledger Fabric

The Linux Foundation used Hyperledger. The permissioned blockchain known as Hyperledger Fabric determines the access level for its users, called peers. Only a small set of people can create transactions and write to the ledger in this.

A different group will be able to check the accuracy and legitimacy of transactions and take part in group consensus. By applying the BTF, or byzantine false tolerance protocol, among all blockchain nodes, the collective agreement is accomplished. Increased security, better work distribution among peers, greater parallelism and synchronisation, and a decrease in bottlenecks are all benefits of the Hyperledger Fabric platform. Additionally, using smart cards decentralises the essential certification services, enhancing data or document reliability, accuracy, and privacy.

Smart contracts

A cryptographer Nick Szabo in 1997 firstly used the term smart contract to create a distributed ledger. Smart contracts are completely digital and offers the same function which is offered by the real world contracts. Smart contracts are actually a small piece of code that is stored on blockchain network, moreover it is like a digital agreement between the members which are associated with the blockchain network. It controls the transactions and its execution which are performed on blockchain network. Transactions performed by using smart contracts are traceable as well as irreversible. Smart contacts provides trusted transactions between unknown numbers without involving the third parties. Smart contacts offers more benefits when deployed with blockchain platform to the different areas for example they are used in banks for loans and automatic payments on delivery, Insurance companies for process claims, as well as in postal companies for payment on delivery etc. Smart contracts are immutable and distributed in nature.

4. ARCHITECTURE

This section explains how the blockchain infrastructure actually operates and how certificate verification is accomplished using the blockchain and smart contracts. Here is a framework that provides certifications or secret documents with privacy, security, accessibility, availability, and consistency. Smart contact cannot be edited or amended once it is deployed in blockchain. In comparison to the conventional format and Stipend cost, time latency is decreased due to process automation. According to Hong Su, by using conventional format the time latency is 52 seconds and by using smart contract the time latency is 40-80 seconds. The proposed Framework uses smart contracts on a permissioned blockchain ledger to exchange student certificates across universities and organizations.

The steps are as follows:

1. Send a request on a network that is privately developed by universities or other organizations with a valid name and domain to gain access to the blockchain membership.

2. With the aid of Smart contracts monitoring, network members evaluate applications submitted by applicants.

3. By enrolling in the affiliated universities, students can access this portal.

4. The certificate or other necessary credentials are placed on the blockchain ledger after each course has been evaluated and successfully completed.

5. The student can send a view request for the papers they have placed in the ledger as long as they are registered users of the university and are connected to the network.

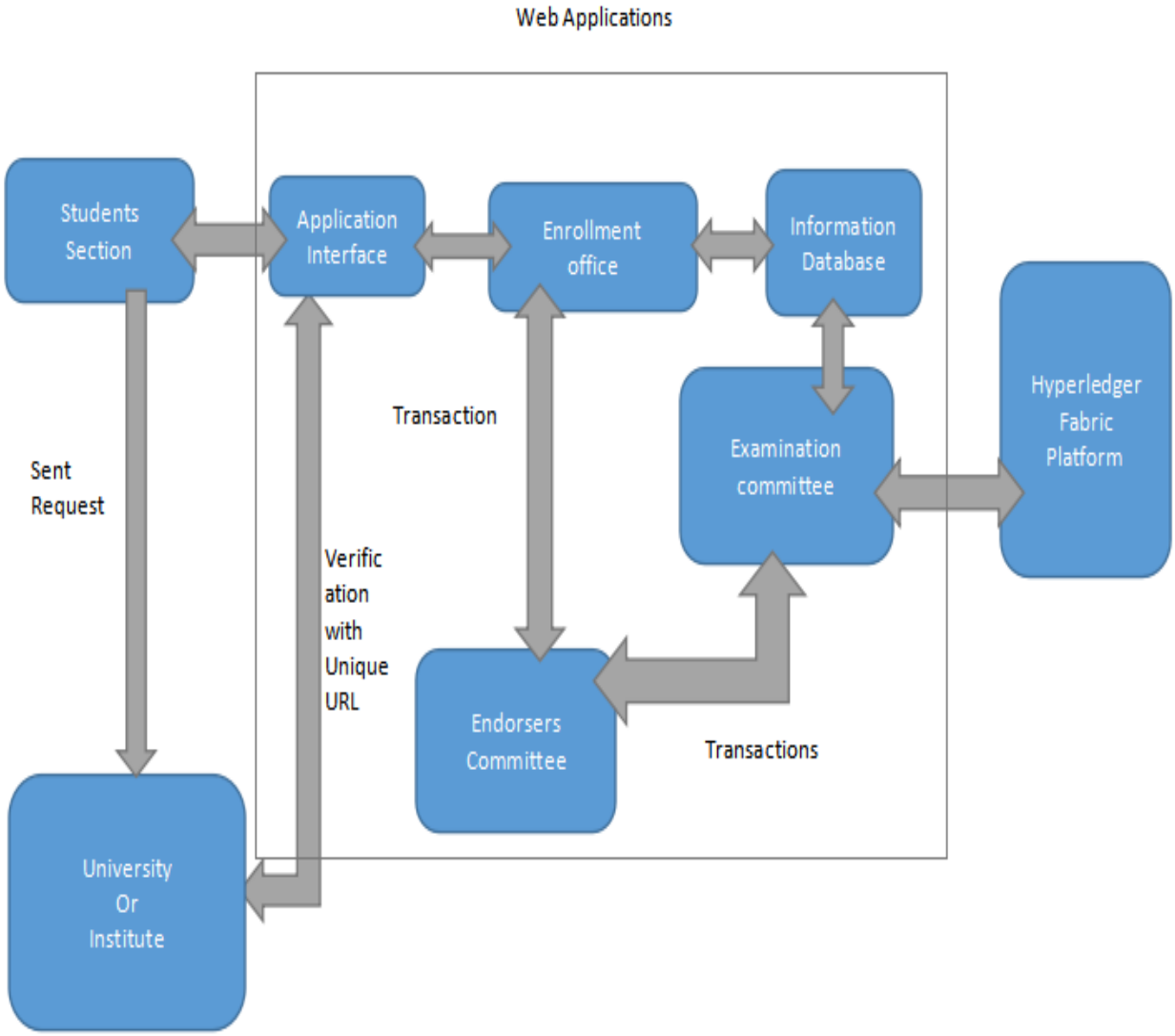

Figure 1 Architecture of Proposed Framework

The technique is broken down into three major sections, which are as follows:

A. Academic certificate issuers have joined the network.

Since they are the only ones who can enter entries into the ledger, the legitimacy of the issuers is crucial. It won't permit unidentified Peers to join the network because it is a permissioned blockchain. Institutions can only join the system using the appropriate internet domains since the administrator has provided a list of universities that is originally valid in the smart contracts.

The institution wants to join the blockchain network, so it creates its address, public keys, and private keys using its blockchain wallet.

Here, the process is carried out by actual access levels interacting with one another. Since this is a private blockchain, only a small number of Peers—referred to as endorser peers—have the authority to execute transactions and add entries to the blockchain's ledger. Each of these Peers must have a

smart contract implemented and maintain full access to all records. Another group of participants, known as committer Peers, will only be able to confirm the legitimacy of transactions and take part in group consensus. Members of this group are not required to install smart contracts, but they must keep the whole record.

Numerous benefits are provided by this approach, including improved work and peer balance, parallelism and synchronisation, and the elimination of bottlenecks. A channel can be used as a component of a procedure between two or more network members for the purpose of confidential transactions thanks to the use of the Hyperledger fabric platform. The network's associated participants must set up smart contracts and blockchain network nodes during the process.

B. Student registration and course

1.The two key processes connected to the transactions are student course completion and registration into the academic system.

2.An applicant's unique ID and a new multi-signature block chain are produced for him or her when they decide to enrol them in a certain university or institution. After that, the two of them are integrated and saved in the current database.

3.Smart contracts are also used for monitoring, which gives the system security measures. In the proposed framework, a multi-stage method to validation is employed to validate the certificates.

4.The danger of data loss or destruction by malware is decreased by making sure the keys are generated and stored on distinct nodes.

5. However, in this case, the applicants cannot identify the proprietors of the signatures. Through this process, transactions were carried out via the decentralised system using smart contracts and blockchain technology.

6.Following a successful transaction, smart contracts are periodically used to update student profiles and ledgers. To secure the digital information, smart contracts that have been deployed on Hyperledger fabric platforms retain the certificates' hash values.

7.The administrations in charge of those individual universities or institutions are normally in charge of creating and updating student profiles any of the malware eradicated.

8. However, in this case, the applicants cannot identify the proprietors of the signatures. Through this process, transactions were carried out via the decentralised system using smart contracts and blockchain technology.

9.Following a successful transaction, smart contracts are periodically used to update student profiles and ledgers. To secure the digital information, smart contracts that have been deployed on Hyperledger fabric platforms retain the certificates' hash values.

10.The administrations in charge of those individual universities or institutions are normally in charge of creating and updating student profiles.

C. Information verification

With the proposed approach, students can validate their certificates or other papers without contacting the agencies that issued them in the first place. If a student wishes to enrol in a different university, the institution from which the student wishes to transfer will get a request to check any documents or certificates the student currently holds. The blockchain address and multi-signature address chosen by the student are delivered to the destination university together with the redemption script using the

original institution's wallet's multi-signature address. Once the students' claims have been verified, the destination university examines the redeem script to confirm the students' multiple signature addresses.

Then, in order to validate the student's identity, it requests a confirmation mail providing their address. The certificate belonging to that student is checked and certified once the institution has verified the signed message and it has matched with the student's blockchain address. Otherwise, the process stops without producing a result. This makes sure that the file is not tampered with during the process.

5. LIMITATIONS AND ADVANTAGES

1. By aiding in the certificate administration process, blockchain technology has the potential to significantly change the way that education is delivered.

2. The blockchain network's certificate authentication is a highly secure, reliable, and unchangeable process.

3. Its peer-to-peer methodology lays out the working and accessing authority for the network's affiliated members.

4. Even though it has tremendous functionality, it is still not commonly used since people continue to trust in third parties.

5. University must pay mining fees during the initial stage of certificate broadcasting in order for it to be verified on the blockchain network.

6. Applications based on the blockchain technology platform are still in the testing stage.

7. The committee member must keep in mind the private key that is linked with the multi signature stage.

6. CONCLUSION

As a result of this research it is found that along with blockchain technology smart contract and Hyper ledger Fabric, the certificates verification is more secure, reliable and having minimum time latency. The infrastructure of blockchain Technology will benefit the educational Arena in variety of ways. It provides a decentralize tamper proof and secured platform for transactions of documents certifications and other such confidential data. It executes in a much promising way to address fraudulent activities and prevents the sensitive information from getting hacked, altered or faked. Because of decentralization it is more scalable, consensus, immutable and secured approach for maintaining, issuing and verification of certificates and others such confidential documents. Its functionality has tremendous impact on time latency and expenditure on the whole procedure as compared to the traditional way.

REFERENCES

[1] T.Keerthana1,R.Tejaswini2,V.Yamini,K.Hemapriya (2019),"Integration of Digital Certificate Blockchain and Comprehensive Behavior Analysis using QR and Smart Contract" *International Journal of Research in Engineering,Science and Management 2*(3).

[2] Nitin Kumavat1 ,Swapnil Mengade,Dishant Desai (2019),“Certificate Verification System using Blockchain” Jesal Varolia. *International Journal for Research in Applied Science & Engineering Technology* (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887 *Volume 7* Issue IV, - Available at www.ijraset.com ©IJRAS 53.

[3] Arshad Jamal, Rabab Alayham Abbas Helmi, Ampuan Siti Nurin Syahirah, Mariam-Aisha Fatima (2019),"Blockchain Based Identity Verification System **"**, *9th IEEE International Conference on System Engineering and Technology* (ICSET), Shah Alam, Malaysia.

[4] Gunit Malik, Kshitij Parasrampuria, Sai Prasanth Reddy, Dr. Seema Shah(2019),"Blockchain Based Identity Verification Model" ,*IEEE International Conference on Vision Towards Emerging Trends in Communication and Networking* (ViTECoN).

[5] Indri Handayan, Ruli Supriati, Euis Siti Nur Aisyah, Sulistiawati (2020), **"**Proof of Blockchain Work on The Security of Academic Certificates" *The 8th IEEE International Conference on Cyber and IT Service Management* (CITSM 2020) On Virtual.

[6] Masoomeh Bahrami, Alireza Movahedian , Arash Deldari (2020),**"**A Comprehensive Blockchain based solution For Academic Certificates Management Using Smart Contracts,"*IEEE International Conferenceion Computer and Knowledge Engineering (ICCKE2020).*

[7] A.Gayathiri, J. Jayachitra ,Dr. S. Matilda (2020), "Certificate validation using blockchain **"** , *IEEE 7th International Conference on Smart Stru ctures and Systems ICSSS 2020*.

[8] Yu-Te Wang, Chu-Fei Wu, Shang-Pin Ma, Hsuan-Tung Chen, Shih-Ying Chang, Chun-Sheng Li (2020) ,"PDAS: A Digital-Signature-Based Authorization Platform for Digital Personal Data", *IEEE International Computer Symposium* (ICS).

[9] Mahmudul Hasan, Anichur Rahman, and Md. Jahidul Islam (2020), **"**Dist BCVS: A Distributed Secure Block chain based Online Certificate Verification System from Bangladesh Perspective**",***IEEE International Conference on Advanced Information & Communication Technology* (ICAICT2020), Dhaka, Bangladesh.

[10] Iftekher Toufique Imam, Yamin Arafat, Kazi Saeed Alam and Shaikh Akib Shahriyar(2021), "DOC BLOCK:A Block chain Based Authentication System for Digital Documents", I*EEE Thir d International Conference on Intelligent Communication Technologies and Virtual Mobile Netw orks (ICICV 2021).*

[11] Sumithra V, Shashidhara R, Debajyoti Mukhopadhyay, Suneet Kumar Gupta (2021)," Decentralized Accreditation of Educational Attainments using Blockchain",*6th IEEE International Conference for Convergence in Technology* (I2CT) Pune, India.

[12] Hong Su, Bing Guo , Yan Shen, Zhen Zhang, and Chaoxia Qin (2021), " To Delay Instantiation of a Smart Contract to Save Calculation Resources in IoT",Hindawi Wireless Communications and Mobile Computing Volume 2021, Article ID 6666236,https://doi.org/10.1155/2021/6666236,