HYBRID DIGITAL CERTIFICATE MANAGEMENT SYSTEM WITH QR CODE AND IOT INTEGRATED ON HYPERLEDGER FABRIC BLOCKCHAIN

Reference NO. IJME 1392, DOI: 10.5750/ijme.v1i1.1392

Dumpeti Naveen Kumar*, Osmania University, Hyderabad, Telangana, India and **Radhika Kavuri**, CBIT, Hyderabad, Telangana, India

*Corresponding author. Dumpeti Naveen Kumar (Emai): bkomuraiah2022@gmail.com

KEY DATES: Submission date: 26.12.2023 / Final acceptance date: 27.02.2024 / Published date: 12.07.2024

SUMMARY

In contemporary society, management of physical documents such as educational certificates, identity proofs, vehicle registrations, and marriage certificates is an integral part of daily life. However, in present online world, there is a pressing need for digital transformation and the management of these documents. One significant challenge associated with this transformation is the susceptibility of original documents to replication or duplication. This vulnerability is particularly concerning in the case of educational certificates, where fraud is prevalent. Fraudulent activities in the education sector can influence the proliferation of counterfeit educational and skill certificates, posing serious risks to society. For instance, individuals holding fraudulent degrees in professions such as engineering, medicine, law, and pharmacy may lack genuine competence, thereby posing substantial societal harm. To address the issue of certificate oversight and deter forgery, various approaches have been employed. Traditional methods typically involve the use of centralized databases or web servers for certificate storage, which introduces vulnerabilities because they represent single points of failure that leads to forgery and information loss. An optimal solution lies in the adoption of a Blockchain system that leverages a decentralized database structure to enhance data storage capacity and security. Blockchain technology has demonstrated disruptive potential and innovative capabilities across multiple sectors because of its decentralized, transparent, and secure attributes. Its impact spans various domains, including banking, supply chain management, healthcare, education, and finance. Notably, in the education sector, Blockchain technology holds promise in enhancing security, transparency, and efficiency across different educational processes. In this study, we explore existing Blockchain oriented certificate management systems, critically analyze their limitations, and propose a novel hybrid educational certificate management model. The proposed model integrates Hyperledger Fabric, IoT, and 2D Barcode to develop a robust and secure framework for managing educational certificates.

KEYWORDS

Digital certificate, Educational certificate, Smart contract, Smart certificate, Digital signature, Distributed ledger, Blockchain

NOMENCLATURE

IoT	Internet of Things
PoS	Proof of Stake
PoW	Proof of Work
F	Frequency

1. INTRODUCTION

Certificates play a pivotal role in various aspects of human life, serving as tangible evidence of an individual's skills, knowledge, accomplishments, and qualifications. They fulfill several key roles: First, certificates, such as diplomas, degrees, and academic transcripts, serve to authenticate a person's educational attainment and validate their academic achievements. Second, certificates often act as prerequisites for employment, demonstrating that an individual possesses the requisite skills and qualifications for a specific job. Employers frequently demand certificates to verify that candidates possess the necessary expertise and training to excel in particular roles. However, incidents of forgery of Ph.D. certificates from various government and private universities/colleges in India have been reported. Perpetrators use various image editing software tools such as Photoshop, Adobe Light-room, and Corel PaintShop Pro for this illicit purpose.

The Entrustment Document Fraud (EDF) wing of the Central Crime Branch recently uncovered a counterfeit certificate operation that had been in operation for a minimum of three years. In December 2023, the authorities arrested four individuals, two of whom hailed from Andhra Pradesh. Police reports indicate that the culprits had disseminated over 4,000 fraudulent degree certificates in exchange for payment during this period (1). Manual verification of educational certificates is time-consuming,

often taking days or even weeks, and requires a significant amount of workforce force. This represents wasteful allocation of resources in terms of manpower, finances, and time. Moreover, situations may arise where an educational institute that issued a certificate is permanently closed and ceases operations. In such scenarios, there is no authoritative entity at the college to authenticate the certificate's validity.

Traditional methods of certificate storage typically involve centralized servers in which administrators possess full access permissions. While certificates may be encrypted and stored on these servers, administrators may still be capable of deleting or altering the data, even if they do not comprehend the encrypted information. Additionally, servers can be susceptible to technical malfunctions, and physical damage may occur due to natural disasters such as earthquakes or fires. Hence, reliance solely on centralized servers for data storage is untenable. Blockchain technology addresses these challenges through data replication and immutability. It offers several distinguishing features, including being a distributed ledger in which each node synchronizes its ledger copy with others in the network. Information stored on the blockchain is immutable, verifiable, and transparent, enhancing trust and security in certificate management.

A. COMPONENTS OF THE BLOCKCHAIN

1. Network Nodes: These comprise singular computers or devices interconnected within the blockchain network. They maintain a replicated version of the entire blockchain ledger and perform essential roles in verifying and disseminating transactions.
2. Block Assembly: Transactions undergo aggregation into blocks that are securely interconnected through cryptographic methods to form a sequential chain. Each block contains a header containing metadata (such as timestamp, nonce, and the hash of the previous block) along with a list of authenticated transactions.
3. Consensus Mechanisms: Consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS), ensure agreement among network participants regarding transaction validity and blockchain state. These mechanisms mitigate fraudulent activities such as double-spending and uphold the integrity of the ledger.
4. Smart Contracts (Optional): Smart contracts or automated contracts encode agreement terms directly into their code. They autonomously execute when predefined conditions are met, eliminating the need for intermediaries. Platforms such as Ethereum are commonly associated with smart contracts.
5. Decentralized Framework: The blockchain operates on a decentralized network of nodes, devoid of centralized control. This decentralized architecture enhances security, reduces censorship risks, and fosters trust among network participants.
6. Cryptographic Protection: Cryptographic hash functions reinforce data security and interlink blocks in a tamper-resistant manner. Each block contains the hash of its predecessor, ensuring the immutability of the blockchain.

B. ARCHITECTURE AND LIFE CYCLE OF BLOCKCHAIN

Blockchain comprises a sequence of interconnected blocks containing diverse information. A block N comprises transaction information, Merkle tree root, hash of N-1 block, and timestamp . Bitcoin, introduced in 2009 by an anonymous single identified as Satoshi Nakamoto, operates as the public ledger for cryptocurrency transactions (2), functioning within a blockchain framework.

The Blockchain facilitates a decentralized ledger available to network peers, wherein recorded data remains resistant to modification. This attribute of immutability is sustained through the concatenation of blocks, hashes, and a consensus mechanism. Each block holds data, its current hash, and the hash of the preceding block. The specific data incorporated in the block differs on the employed Blockchain variant. For instance, in Bitcoin, a block encompasses transaction details such as transaction lists, hashes, and block headers. Bitcoin stands as the pioneering Blockchain, often serving as the standard for discussing Blockchain architecture. The term ”Genesis Block” signifies the initial block of any Blockchain.

Participants transmit transactions to the Bitcoin network, including sender and receiver information, amounts, and other relevant data. Miners, which are specialized nodes within the network, aggregate these transactions into blocks. Subsequently, miners embark on a vigorous endeavor to solve intricate mathematical puzzles, commonly known as the ”hash puzzle,” necessitating substantial computational resources. The consensus process within the Bitcoin Blockchain is governed by a mechanism called Proof of Work (PoW).

C. OUTLINE OF OPERATION

1. Transaction Propagation: Participants within the Bitcoin network disseminate transactions containing the sender, recipient, amount, and other relevant details.
2. Mining: Miners, specialized network nodes, collect these transactions and organize them into blocks. They then participate in solving a complex mathematical puzzle, known as the ”hash puzzle,” requiring significant computational power.
3. Proof of Work: Miners allocate computational resources to repeatedly hash the block's data with a randomly generated nonce, searching for a hash value that meets specific difficulty criteria. The network adjusts the puzzle's difficulty dynamically to maintain

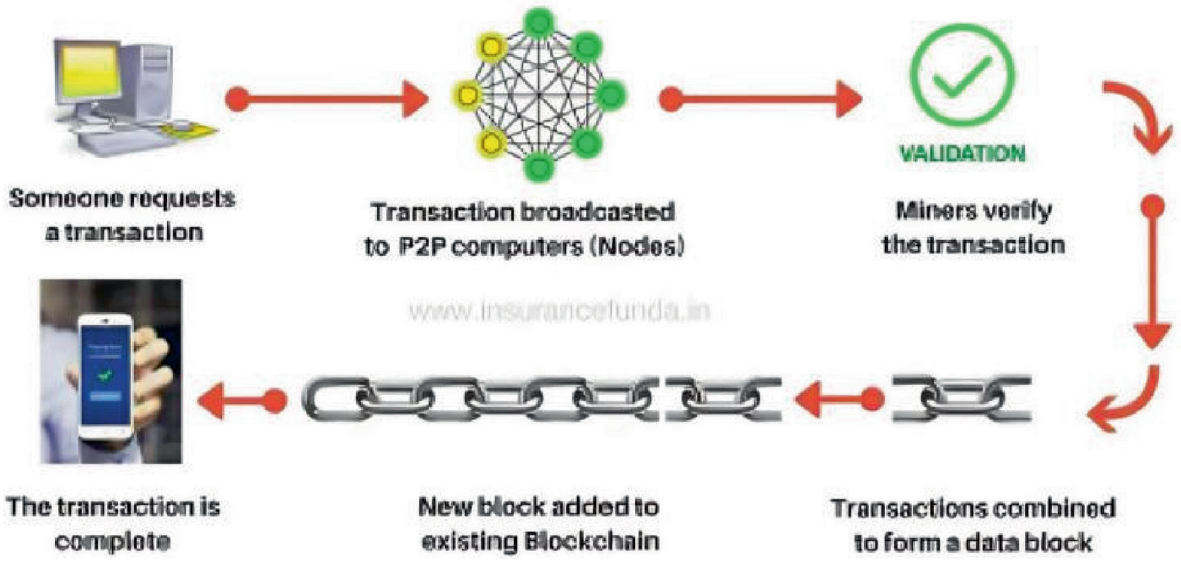

Figure 1. Blockchain life cycle

an average mining rate of approximately one block every 10 minutes.

4. Validation: Upon finding a solution to the hash puzzle, a miner shares the newly formed block with the network. Validators and other nodes scrutinize the block and its transactions for legitimacy. They verify that transactions adhere to the consensus rules outlined in the Bitcoin protocol, ensuring factors such as the validity of digital signatures and the absence of double-spending.
5. Consensus: If the majority of network nodes agree on the block's validity and acknowledge the miner's completion of the required computational work (Proof of Work), the block is added to the blockchain. The blockchain with the highest cumulative Proof of Work is considered valid, with nodes consistently opting for the longest legitimate chain. This mechanism ensures consensus among all network nodes regarding the blockchain's status and transaction sequence.
6. Block Reward: In recognition of their efforts, miners receive newly generated bitcoins along with transaction fees from the block they successfully mined. This incentivizes miners to commit their computational resources to bolstering the network's security.

A user can initiate a Bitcoin transaction by sending a portion or Bitcoin's entirety through its native Blockchain. This process involves aggregating such transactions into a block. When a block reaches its capacity, upcoming latest transactions are stored in a new block(?). As depicted in Figure 1, the accumulated transactions are propagated throughout the Bitcoin network and are collected by mining nodes (4). The miner compiles the accumulated transactions into one single Block and employs the algorithm to solve the puzzle. Upon successfully solving the puzzle, the winning node broadcasts its solution to the rest of the nodes in the network. The linking of a latest block to the Blockchain occurs after validation of transactions.

2. LITERATURE SURVEY

A. LIMITATIONS OF THE CONVENTIONAL CERTIFICATES STORING MECHANISM

The fact that organizations have to invest a lot of effort in manually confirming professional and educational credentials shows how poor the current certificate management systems are at preventing forgeries. A great deal of forgeries have happened with regard to different kinds of documents, such as study certificates, health certificates, land documents, and professional certificates. Since all the data in traditional centralized database systems is kept on a single machine, it is vulnerable to corruption and tampering. Although keeping encrypted copies of certificates in the database improves security, there are still weaknesses because database administrators have the power to add, remove, or modify data. Maintaining several data replicates across multiple servers can help to improve reliability by providing a means of restoration in the case of data loss or failure. Robust verification systems that provide verifiability, immutability, and transparency have a flaw. Global reports of certificate forgeries are a constant reminder of how urgently we need a trustworthy way to distribute and keep certificates securely while guaranteeing data immutability.

B. BLOCKCHAIN FOR CERTIFICATE MANAGEMENT

Instances of forgery span various document types, including health documents, study certificates, land registration

documents, and career documents. Organizations invest considerable time in manually verifying educational and Skill certificates, revealing the inefficiency of current certificate management methods in combating forgery.

In classic centralized database systems, all data reside on a single machine, rendering it vulnerable to tampering or corruption. Despite storing encrypted versions of certificates in the database to enhance security, vulnerabilities persist as database administrators retain the authority to modify or erase information. To bolster reliability, it is advisable to maintain multiple replicas of data across several servers, facilitating restoration in the scenario of data loss or node failure.

Initially introduced as Bitcoin's payment system in 2009, Blockchain has since evolved, spawning platforms like Ethereum, which enable the development of decentralized applications across various domains such as land registration, education, finance, healthcare, and banking. Ethereum is the first ever Blockchain that introduced smart contracts on a public Blockchain. Ethereum facilitates Decentralized application development with the support of Solidity. Ethereum encompasses PoW initially but later migrated to PoS algorithm(5). These systems find utility in verifying certificates for employability, higher education, and career progression in daily life scenarios(6). Blockchain comes in various forms including public, private, and consortium Blockchains, all facilitating decentralized and distributed ledger storage.

The benefits of blockchain technology include:

1. Prevention of Certificate Forgery: Blockchain ensures that applicants with genuine talent, skills, and qualifications gain admission to educational institutions by preventing certificate forgery.
2. Expedited and Cost-Effective Verification: Companies benefit from expedited and cost-effective verification and recruitment processes facilitated by blockchain technology.
3. Future Accessibility: Blockchain data will remain accessible for modification and tracking purposes in the future, enhancing data management and transparency.
4. Immutability of Information: Information stored in the backchain ledger is immutable due to existing processing power limitations, ensuring data integrity and reliability.
5. Use of Cryptographic Techniques: Blockchain utilizes cryptographic techniques such as encryption/decryption, hashing, and digital signatures for permanent certificate storage, enhancing security and privacy.
6. Secure Access: Secure access to certificates is ensured through private keys, which provide individuals with control over their own data.
7. Decentralized Verification: Verification is done by a random peer in the network, promoting decentralization and transparency in the verification process.
8. Reduced Verification Costs: Blockchain technology guides to a drastic reduction in certificate verification costs as third-party involvement becomes unnecessary, streamlining processes and saving resources.

C. EXISTING BLOCKCHAINS: BITCOIN, ETHEREUM, AND MULTICHAIN

We will try to identify an optimal environment that meets current requirements while maximizing benefits from the Blockchain ecosystem. A diverse range of Blockchain platforms is available in the market to tackle this challenge and facilitate the development of the required systems. The Bitcoin Blockchain, which is renowned as the pioneering Blockchain, operates as a payment system with its native cryptocurrency. While its primary focus remains on Bitcoin transactions, it retains the capabilities for Bitcoin scripting, enabling the development of smart certificates. However, Bitcoin faces scalability issues due to its 1 MB block size constraint and incurs costly transaction fees and processing power requirements due to its Proof of Work consensus algorithm.

In contrast, Ethereum emerges as the inaugural blockchain platform that supports smart contract programming and utilizes a Proof of Work algorithm for consensus. Nonetheless, Ethereum suffers from high transaction fees borne by transaction initiators for every write operation on the blockchain (7). Although reading data from Ethereum does not incur transaction fees, it lacks privacy mechanisms and access permissions, rendering it unsuitable for our requirements.

Another alternative blockchain, Multichain, lacks support for smart contracts crucial for automating tasks among network stakeholders. The University of Nicosia (UNIC) pioneered the management of academic certificates on the Blockchain. UNIC utilized the Bitcoin Blockchain as a platform for certificate storage and verification, albeit incurring transaction fees in terms of the cryptocurrency Bitcoin (8).

D. BLOCKCHAIN-BASED CERTIFICATE MANAGEMENT SYSTEM COMPARISON

Using smart contracts for certificate production, the Ethereum-based blockchain system (IEEE Access, 2020) was created on the permissioned blockchain of Ethereum (9). All information included in smart contracts is accessed exclusively through the CertManage Contract, and certificate templates are updated and maintained as

needed. Unfortunately, the system has slow transaction speeds (15 transactions per second) and charges a high transaction cost of 7 to 30 worth of Ether, believing on network demand for data storage on the blockchain.

To store certificates off-chain and maintain certificate information on the Blockchain, EduRSS presents a Secure Storage and Sharing Scheme for records (10). It uses a centralized storage server for off-chain storage and is based on the public backchain Ethereum, which raises security concerns. demand for data storage on the blockchain, and demonstrates slow transaction speeds (15 transactions per second). On the blockchain, there is a hefty transaction charge in terms of Ether associated with each transaction (record storage).

A method for granting and confirming educational certifications is called EUniCert (11). A frontend is used by users to communicate with the EUniCert system, while a Backend connects to the EUniCoin network to generate certificates inside the EUniCoin system. To facilitate operations like retrieval, verification, and issuance, this process comprises producing transactions and placing them into blocks.

EduCTX functions as a mechanism that stores certificates on the public backchain network, Ark (12). Students accumulate ECTX tokens after receiving certifications; they should have enough tokens to finish their studies. Students can provide businesses or universities with their backchain address to worldwide authenticate their finished courses.

Smart contracts are used by DIGICERT, a safe decentralized application, to store data in the ledger (13). With its foundation in the public Ethereum blockchain, it

Table 1. Comparison of different blockchain-based certificate management systems

System	Blockchain Used	Advantage	Disadvantage
EuniCert: An Ethereum-Based Digital Certificate Verification System	Ethereum	Better performance than the previous Unicert system. Built on the Ethereum blockchain	Payment of the certificate generation fee in terms of Eunicoin
Ethereum-based Smart Contract Certificate System	Permissioned Ethereum	Ethereum backchain is the platform that is being used. Certificate creation is done via smart contracts.	Variable transaction fee of Ether from 7 to 30 worth of Ether to store data on backchain
EduRSS	Ethereum	Has the capacity to manage hundreds of entities. Members' defined access permissions	Certificates are stored off the chain. Loss of certificates.
Hyperledger-based Framework for Educational Certificates management	Hyperledger Fabric	Private Blockchain using Hyperledger Fabric	Only prototype specified, no implementation
DIGICERT	Ethereum	A one-time password is used for authentication of the user. QR code used for certificate verification	High transaction fees in terms of Ether
EduCTX	Ark	Wallet provided. After completion of the course, each student receives ECTX tokens to the wallet address	Ark is a permissionless blockchain that anyone can join. No authentication of members. 15 transactions per second are processed
Blockcerts	Bitcoin	Provides an API that can be used by other applications	High transaction fee, 7 transactions per second are processed. No built-in smart contracts
Smart Contract-based Blockchain for Certificate management	Ethereum	Use of QR code for easy verification	High transaction fees in terms of Ether

serves as a document manager. QR codes make certificate verification easier. Based on application events, Ethereum smart contracts are used to create rules that regulate nodes within the peer-to-peer network. A one-time password approach is used to verify users' identities.

Documents can be entered into Smartcert, which then creates a digital certificate and hash to be stored on the blockchain (14). The produced hash is used by users to access the certificate. Users may find it difficult to preserve the hash. It might not be a safe way to exchange credentials, even though individuals can share the hash with employers on the blockchain network to confirm the legitimacy of the certificate.

Blockcerts, employed by universities such as the University of Nicosia and the University of Birmingham (15), enable the maintenance of educational certificates on the blockchain. Blockcerts uses the Bitcoin public blockchain to generate and store digital documents. Distributed applications developed using Blockcerts allow the management of academic and professional certificates.

The MIT Media Lab uses Blockcerts to create and verify educational certificates (16). However, there is a need for better privacy mechanisms for accessing data on the blockchain. Blockcerts eliminates third-party involvement in certificate management by providing better control over certificates. Nonetheless, privacy for recipients in terms of certificate visibility is not adequately addressed.

4. PROPOSED MODEL

The methodologies discussed in the previous sections rely on open platforms such as Bitcoin and Ethereum. However, these platforms often lack the authentication, privacy features, and fine-grained access permissions necessary for secure certificate retrieval. In response, our proposed model provides stakeholders with enhanced access privileges, thereby ensuring improved security and cost efficiency compared to existing approaches. To achieve a more sophisticated level of access control, our model uses a Hyperledger Fabric-based permissioned blockchain framework, which is further augmented with IoT integration and the utilization of two-dimensional barcodes (17). This combination offers employers a flexible means of accessing certificates while maintaining robust security measures.

Within the Hyperledger Fabric framework, the transaction process follows several distinct phases:

1. Transaction Proposal Initiation: The client kick-starts a transaction proposal by endorsing it with the user's certificate and then dispatches the proposal to a group of endorsing peers.
2. Endorsement and Simulation: Each endorsing peer simulates the transaction, generating a resultant read-write set. The endorsed proposal is subsequently transmitted back to the client.
3. Verification and Forwarding: The client verifies the endorsed proposal acknowledgements and forwards the transaction, along with the endorsed proposal responses, to the orderer.
4. Ordering and Block Formation: Upon receipt, transactions are sequenced and a new block is formed by the orderer.
5. Validation and Versioning: The orderer disseminates the new block to all peers. Each peer ensures that the block is signed by the requisite minimum number of endorsing peers as per the endorsement policy. Subsequently, a versioning check is conducted, marking transactions as either valid or invalid. If valid, the world state is updated accordingly.
6. Blockchain Appendage: Finally, the received block is appended to a node's local blockchain.
7. Transaction Notification: The client receives notification regarding the transaction's success or failure.
8. Permissioned Access: Granular permission levels and precise access control are made possible by Hyperledger [18].

5. METHODOLOGY

A network is established with stakeholders Universities, Colleges, and students as depicted in Fig. 2. Client API is developed and used to store students' information on a blockchain. API is also used to scan QR code and download the student's certificate.

A. HYPERLEDGER FABRIC ADVANTAGES

- Authentication: By usage of digital certificates provided by a certificate authority, stakeholders can access a channel. The certificate authority could be Fabric's default or that of a different organization.
- Throughput: Compared with other blockchains, Hyperledger exhibits better throughput, execution time, and latency.
- Transparency: All organizations share a single channel that synchronizes a unified ledger. It is possible to create multiple channels, and only approved organizations are allowed to join. Additionally, a company could be a part of several channels.

The coordinator registers college/university as shown in Fig. 3. Students' personal information such as name and email along with college/university are recorded on Blockchain as shown in Fig. 4. Students' fingerprints are also stored on Blockchain along with personal information. Fig. 5 depicts the NodeMCU Fingerprint module used to store student fingerprints on a blockchain.

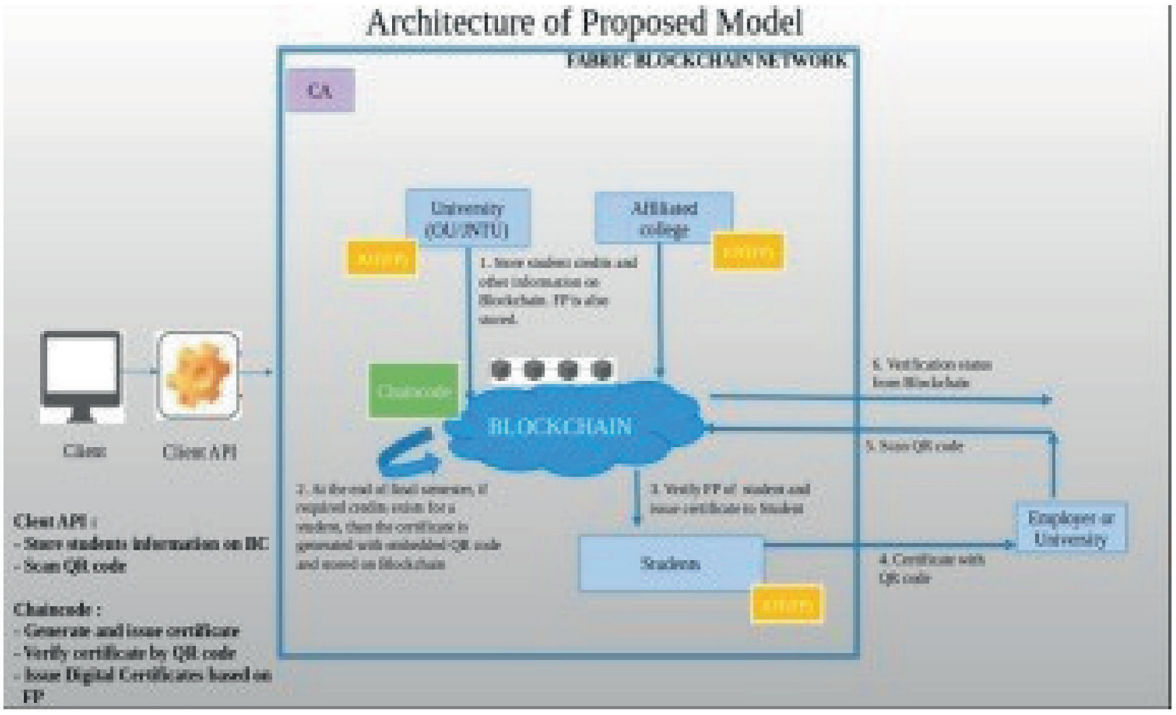

Figure 2. Architecture of the proposed hybrid certificate management system

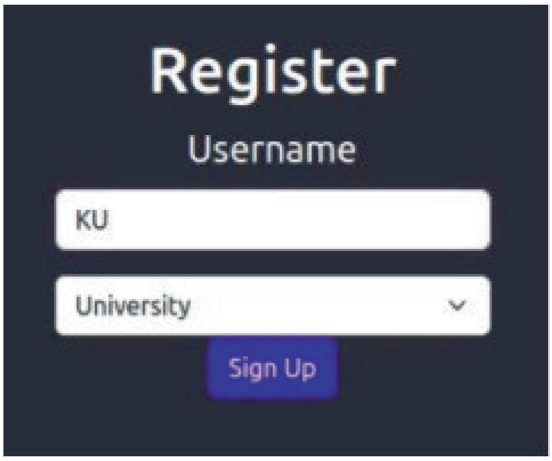

Figure 3. University/college registration

Figure 4. Student registration

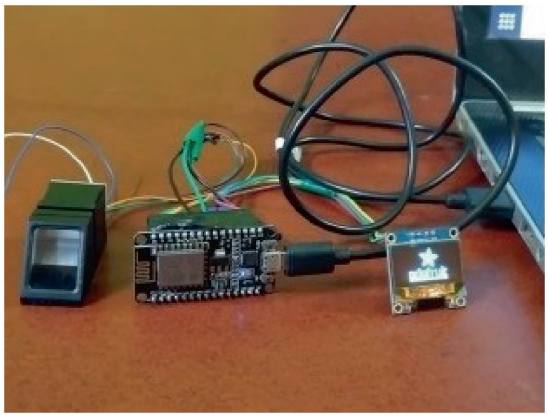

Figure 5. NodeMCU ESP8266 kit

Registered student details can be accessed by the coordinator using the student registration number, as shown in Fig. 6. Based on the marks obtained, the required number of credits are calculated. A student with a backlogs may not achieve the required number of 144 credits. At the end of the last semester, if the total number of credits are equal or greater than 144 credits, the certificate is successfully generated with the student registration number, as shown in Figure 7. The QR code is generated based on the hash of the certificate. Finger print of student is verified with NodeMCU and final certificate is issued to student. So only the respective student will receive the final certificate. A student may provide a hard copy or a soft copy of their certificate to a higher education institution, the company, or both during an interview. By simply scanning the QR code

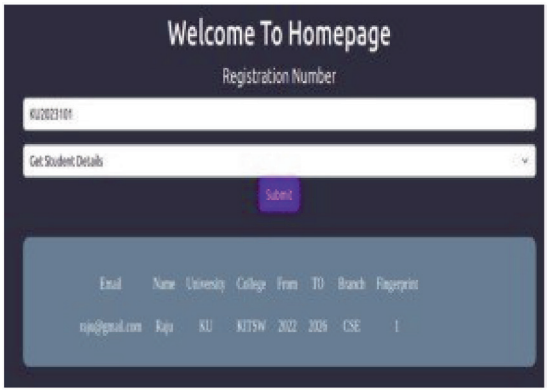

Figure 6. Student registered details

Figure 7. Generate certificate

on the certificate, officials can access the certificate as shown in Fig. 8.

5. PERFORMANCE EVALUATION

Current methods for managing certifications use ARK Blockchains, Ethereum, and Bitcoin. Table II indicates that the block creation time for these blockchains is high.

The proposed platform is based on Hyperledger Fabric, which has a high transaction rate per second compared with all other Blockchains. Bitcoin has a high transaction fee when taking these fees into account. Because Fabric is a private blockchain, there are no transaction fees.

Figure 8. Certificate with QR code

Table 2. Transaction speeds and fees incurred in various Blockchains

Blockchain	TPS	Transaction Fee
Bitcoin	7	$4
Ethereum	30	$13
ARK	15	$0.189
Hyperledger Fabric	Up to 3000	No transaction fee

Hyperledger Caliper is used to evaluate the performance of the system.

The number of virtual institutions is simulated by generating parallel threads of execution in numbers of 200, 400, 600, and 800 virtual institutions, and the execution time is noted. This simulation helps assess the scalability and efficiency of the proposed platform under varying loads. Figure 9 shows Architecture of the proposed hybrid certificate management system.

Reaction time is indicated on the Y-axis in intervals of 5k ms, while the number of virtual institutions is indicated on the X-axis. The minimum, average, and maximum time consumed by the virtual institutions to generate the certifications are plotted on the graph (see Figure 10).

The average transaction speeds for different numbers of virtual institutions generating certificates are as follows:

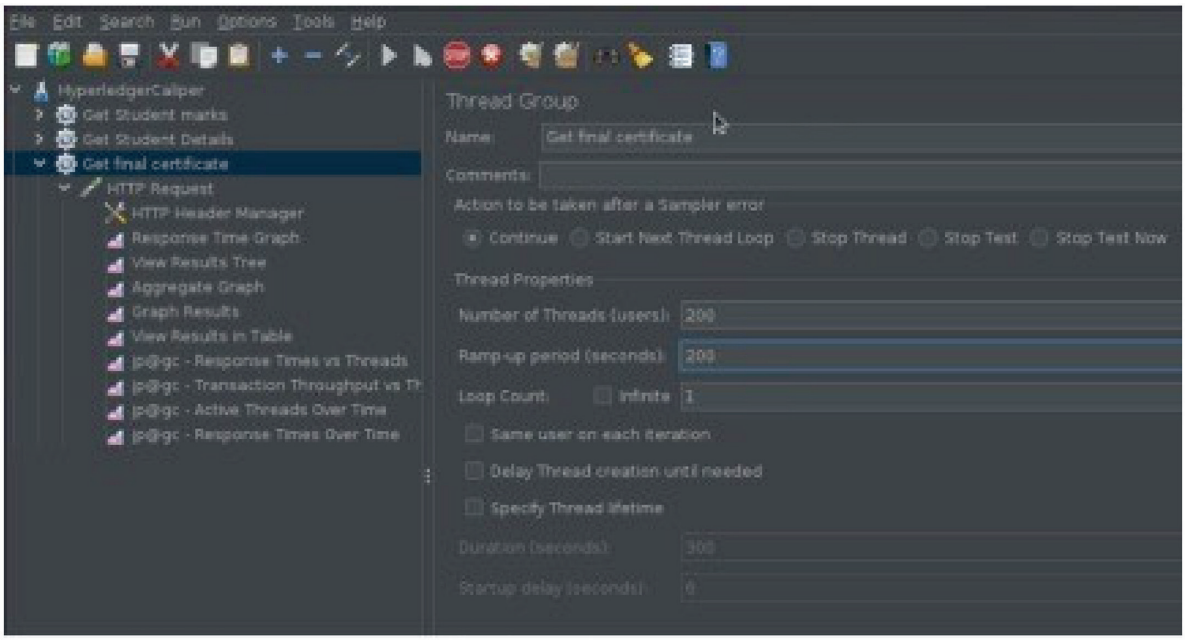

Figure 9. Architecture of the proposed hybrid certificate management system

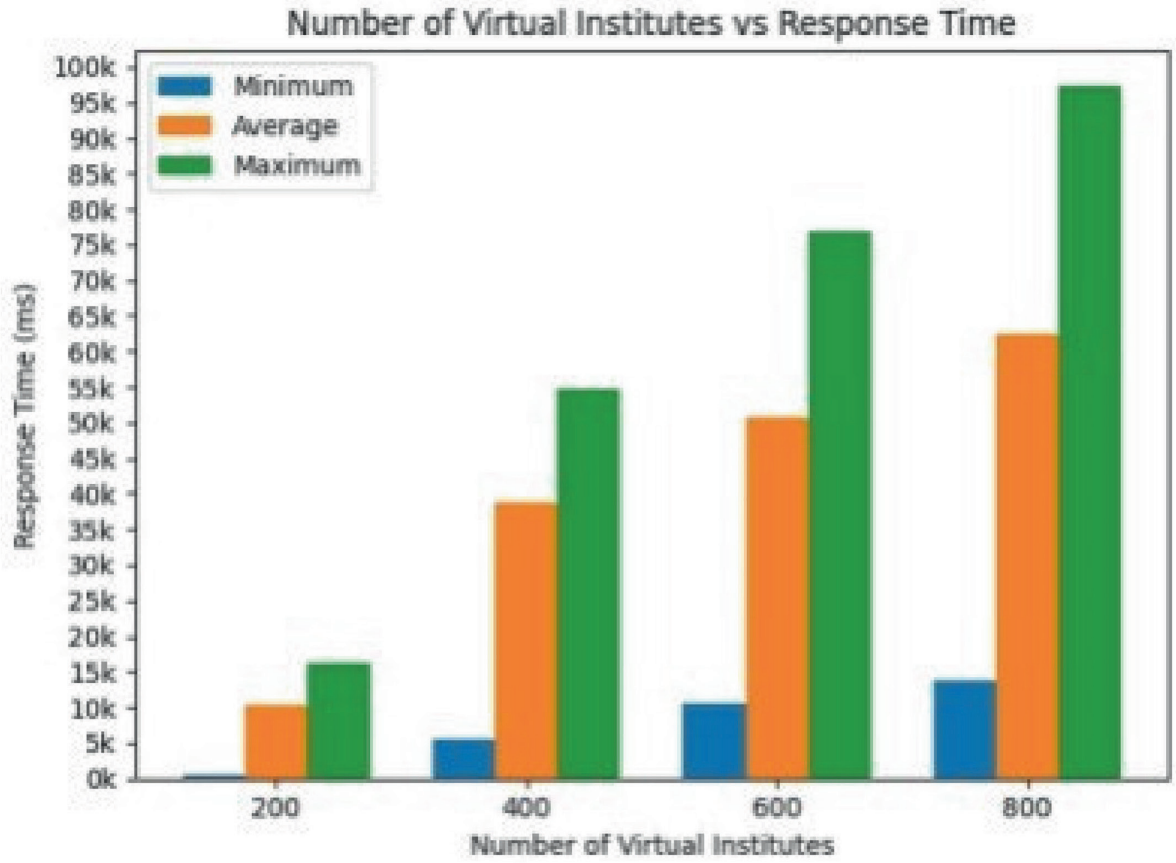

Figure 10. Graph representing the minimum, average, and maximum time consumed by virtual institutions

- 200 virtual institutions: 522 ms
- 400 virtual institutions: 5470 ms
- 600 virtual institutions: 10461 ms
- 800 virtual institutions: 13648 ms

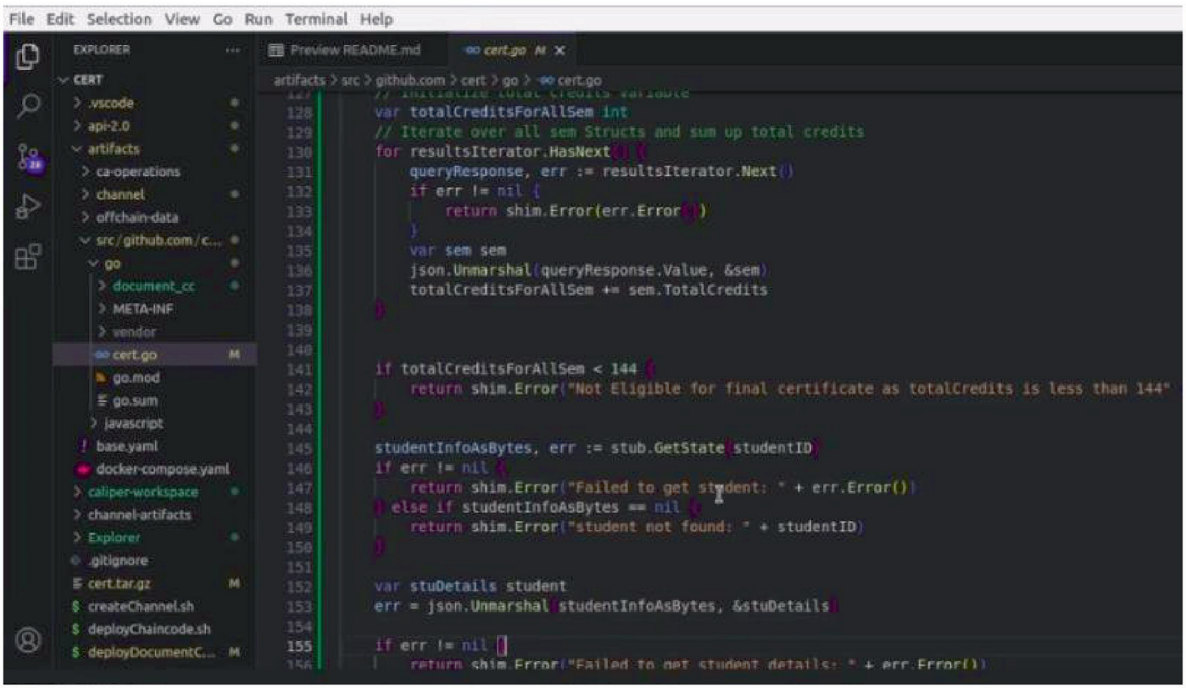

Figure 11. Certificate go code snippet considering the scenario with 800 virtual institutions

and an acknowledgment time of 13648 ms, the performance of our system can be calculated as follows:

Performance = Number of transactions/Response time

Number of transactions = 800 (number of virtual institutions) Response time = 13648 ms

Performance = 800/13648 ms ≈ 0.058 transactions per millisecond

Converting this to transactions per second:

Performance ≈ 0.058 transactions per millisecond×1000 ms ≈ 58 transactions per second

Therefore, the performance of our system in the scenario with 800 virtual institutions is approximately 58 transactions per second. Figure 11 shows Certificate go code snippet considering the scenario with 800 virtual institutions.

6. CONCLUSION AND FUTURE WORK

In conclusion, the implementation of a permissioned blockchain system has demonstrated its effectiveness in enhancing security, access permissions, and the streamlined management of educational documents. By leveraging cryptographic techniques such as hashes and digital signatures, the system ensures the integrity and immutability of educational certificates, effectively mitigating the risks associated with data manipulation or forgery. Through the use of a permissioned blockchain, the system provides a robust and foolproof method for preserving educational certificates, instilling confidence in the authenticity and validity of academic credentials. Looking ahead, there are several avenues for future work and enhancements to further advance the capabilities of the system. First, continued research and development efforts can focus on refining the permissioned blockchain framework to optimize performance and scalability, thereby accommodating a larger volume of educational documents and users while maintaining efficient transaction speeds.

Moreover, the expansion of the system's functionality to include other important documents such as identity cards represents a promising direction for future work. By extending the framework to encompass identity verification and authentication, the system can serve as a comprehensive solution for securely managing personal credentials in various contexts, thereby enhancing overall security and efficiency in identity management processes. Furthermore, exploring novel technologies such as zero-knowledge proofs or advanced encryption techniques could further enhance the privacy and security features of the system, ensuring that confidential information remains protected while still facilitating seamless verification processes.

Overall, the novel system represents a significant advancement in the field of document management, particularly within the educational sector. Through ongoing research and innovation, it has the potential to revolutionize the way educational credentials and other important documents are stored, shared, and verified, ultimately benefiting individuals, educational institutions, employers, and other stakeholders.

ACKNOWLEDGMENT

The researchers from the AU College of Engineering (A), located in Visakhapatnam, AP, are highly valued for their contribution to this research.

FUNDING STATEMENT

Not applicable.

ETHICS APPROVAL

Not applicable.

CONFLICTS OF INTEREST

No conflicts of interest.

DATA AVAILABILITY

Not applicable.

CONSENT TO PUBLISH

Nil.

7. REFERENCES

1. Times of India. "Fake Degree Certificate Network Busted; Four Arrested by City Police, Probe On." Times of India.
2. Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." *www.Bitcoin.org*, 2008, p. 9.
3. Puthal, D., Malik, N., Mohanty, S.P., Kougianos, E., Yang, C. "The Blockchain as a Decentralized Security Framework (Future Directions)." *IEEE Consum. Electron. Mag.* 7(2), 18–21 (2018).
4. "Bitcoin Cryptocurrency." Insurance Funda.
5. Buterin, Vitalik. "A Next Generation Smart Contract & Decentralized Application Platform." 2018.
6. Lizcano, David, Lara, Juan A., White, Bebo, Aljawarneh, Shadi. "Blockchain-based Approach to Create a Model of Trust in Open and Ubiquitous Higher Education."
7. Chen, Jiin-Chiou, Lee, Narn-Yih, Chi, Chien, Chen, Yi-Hua. "Blockchain and Smart Contract for Digital Certificate." *IEEE ICASI*, 2018.
8. "Academic Certificates on the Blockchain." UNIC Blockchain Initiative, 2018. [Online]. [Accessed: 13/03/2020].
9. Xie, Rui, Wang, Yuhui, Tan, Mingzhou, Zhu, Wei, Yang, Zhongjie, Wu, Jiaji, Jeon, Gwanggil. "Ethereum-Blockchain-Based Technology of Decentralized Smart Contract Certificate System." *IEEE*, 2020.
10. Li, Hongzhi, Han, Dezhi. "EduRSS: A Blockchain- Based Educational Records Secure Storage and Sharing Scheme." *IEEE Access*, vol. 7, 2019.
11. Huynh, Trong Thua, Pham, Dang-Khoa. "Eunicert: Ethereum Based Digital Certificate Verification System." *International Journal of Network Security Its Applications (IJNSA)*, Vol. 11, No.5, September 2019.
12. Turkanovic, Muhamed, Holbl, Marko, Kosic, Kristjan, Hericko, Marjan, Kamisalic, Aida. "EduCTX: A Blockchain-Based Higher Education Credit Platform." *IEEE*, 2018.
13. Poorni, Ms. R., Lakshmanan, Mr. M., Bhuvaneswari, Ms. S. "DIGICERT: A Secured Digital Certificate Application using Blockchain through Smart Contracts."
14. Kanan, T., Obaidat, Ahamd Turki, Al-Lahham, Majduleen. "SmartCert BlockChain Imperative for Educational Certificates." *IEEE*, 2019.
15. "Blockcerts: An Open Standard for Building Apps." Blockcerts, 2018. [Online].
16. MIT Media Lab. "What We Learned from Designing an Academic Certificates System on the Blockchain." MIT Media Lab.
17. Husain, A., Bakhtiari, Majid, Zainal, Anazida. "Printed Document Integrity Verification Using Barcode." eISSN 2180–3722, 99-106, 2014.
18. "Hyperledger Fabric Peers." Hyperledger Fabric Documentation.

