

Enhancing Educational Certificate Verification With Blockchain and IPFS: A Decentralized Approach Using Hyperledger Fabric

Rafah Amer Jaafar¹, Saad Najim Alsaad¹

¹Department of Computer Science, College of Science, Mustansiriyah University, Baghdad, Iraq

Abstract – Educational certificate counterfeiting poses a significant global challenge, demanding urgent attention and robust solutions. This paper addresses the problem of forgery and verification of educational certificates by leveraging blockchain technology as an anti-counterfeiting measure. A decentralized architecture for educational certificate verification systems is proposed and implemented using the Hyperledger Fabric as a blockchain platform and the Inter Planetary File System (IPFS). By utilizing the unique features of these technologies, we aim to establish a reliable and secure system for verifying authenticity of educational certificates without relying on third-party intermediaries. Our approach involves storing educational certificate files on a decentralized file system, namely IPFS, ensuring their integrity and accessibility. To enable efficient verification, each certificate is associated with a certificate ID, which retrieves the necessary validating information from the Hyperledger Fabric network. This integration ensures that educational certificates are securely stored on the blockchain, preventing any tampering attempts and enabling easy validation. The experimental results demonstrate that educational certificates are stored on the Hyperledger Fabric network in a manner that ensures their immutability, making it impossible to alter them.

DOI: 10.18421/TEM124-51

<https://doi.org/10.18421/TEM124-51>

Corresponding author: Rafah Amer Jaafar,
Department of Computer Science, College of Science,
Mustansiriyah University, Baghdad, Iraq


Email: rafah_amer@uomustansiriyah.edu.iq

Received: 29 July 2023.

Revised: 17 October 2023.

Accepted: 25 October 2023.

Published: 27 November 2023.

 © 2023 Rafah Amer Jaafar & Saad Najim Alsaad; published by UIKTEN. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 4.0 License.

The article is published with Open Access at <https://www.temjournal.com/>

Furthermore, the system allows for verification of their authenticity without the need for any third-party intervention. By combining the power of blockchain technology with IPFS, our solution provides a robust approach to tackle the growing issue of educational certificate counterfeiting. This research contributes to the field by offering a decentralized architecture that enhances the security and trustworthiness of educational certificate verification systems.

Keywords – Educational certificate verification, blockchain, Hyperledger Fabric, inter planetary file system (IPFS), anti-counterfeiting decentralized architecture.

1. Introduction

Educational certificates hold significant value as proof of completing academic stages and play a crucial role in confirming an applicant's educational history for institutes of higher education and companies. Unfortunately, this importance attracts fraudsters who attempt to obtain secure jobs by presenting forged educational certificates. As a result, organizations are burdened with the task of verifying certificates received from applicants, imposing a substantial workload on universities and other institutions [1].

Traditional methods of verifying educational certificates involve manual processes and centralized servers. However, these methods come with limitations, including the labor-intensive nature of manual verification and the vulnerability of centralized systems to hacking [2].

In light of these challenges, blockchain technology presents an intriguing solution for the education field. It offers advantages such as enhanced data management, verification of data authenticity, transparency, streamlined certification procedures, reduced time spent on certificate verification, increased trust, and cost savings [3]. Blockchain provides a secure platform for sharing students' certificates, ensuring data integrity, and increasing transparency.

The purpose of the proposed system is to propose and evaluate a system that leverages blockchain technology for educational certificate verification. Section 2 presented the subsequent sections will delve into related works, section 3 explain the proposed system, section 4 discuss the tools and principles employed, section 5 present experimental results, and section 6 conclude the paper.

By adopting blockchain technology for educational certificate verification, we aim to address the challenges of security, efficiency, and trustworthiness, ultimately contributing to the development of a more reliable and robust system.

2. Related Works

The use of blockchain technology may be found in many different industries, such as the financial sector, the healthcare industry, and the educational sector. The application of blockchain technology in verification systems is currently receiving a lot of interest, despite the fact that it is still in the beginning phases of development. This section provides an overview of the most recent best practices for verifying information.

Prince Waqas Khan *et al.* [4] proposed surveillance camera verification (CCTV) system that is based on blockchain technology in order to determine whether or not adjustments have been made to a video. It helps in distinguishing between real and fake recordings and ensures the validity of security cameras.

Tomasz Hyla and Jerzy Pejas [5] presented a signature verification system utilizing blockchain technology. Their work focuses on signing and validating digital documents using a permissioned blockchain approach.

Binh Minh Nguyen *et al.* [6] introduced the Vietnam Education Certification blockchain (VECEfblock) system, addressing concerns over false credentials in Vietnam. Their system utilizes the Hyperledger Fabric platform, a permissioned blockchain, which was deployed on the Amazon EC2 service.

Jian Wang *et al.* [7] implemented a cellular-connected unmanned aircraft verification system based on blockchain technology. This work aims to enhance the security of cellular connections within the context of unmanned aerial systems.

Jin Wang *et al.* [8] proposed a Merkle tree structure for transaction verification in Industrial Internet of Things (IIoT) systems utilizing blockchain technology. Their approach addresses the specific challenges of IIoT systems and emphasizes the importance of efficient and secure transaction verification.

Elva Leka and Besnik Selimi) [9] developed a blockchain-based application for storing and verifying educational certificates. Their system utilizes smart contracts and the Ethereum platform for certificate storage, while employing IPFS for data storage. AES encryption algorithm is used to provide data confidentiality.

In this paper, we contribute by proposing a decentralized architecture for educational certificate verification, employing the permissioned blockchain platform Hyperledger Fabric and IPFS. Our approach significantly reduces the time and effort required for verification by utilizing a certificate ID to retrieve validation data from the Hyperledger Fabric network.

These related works demonstrate the diverse applications of blockchain technology in verification systems and highlight the potential for enhancing the security, efficiency, and trustworthiness of educational certificate verification processes.

3. Background

In this section, we try to briefly address some of the concepts and tools related to blockchain that are used in the proposed system.

Blockchain technology, at its core, is a decentralized and distributed ledger system that ensures transparency and trust in transactions. It employs cryptographic hashing, consensus mechanisms, and immutability to create a tamper-proof record of data. These features eliminate the need for intermediaries, enhancing security and efficiency in various industries.

In the context of educational certificates verification, traditional systems face issues such as manual processes, centralized servers, and vulnerability to tampering. To overcome these challenges, blockchain technology presents an innovative solution.

In our proposed system, we leverage the capabilities of Hyperledger Fabric platform, as a permissioned blockchain specifically designed for enterprise usage. Hyperledger Fabric provides a scalable infrastructure and secure for educational certificate verification, ensuring data privacy and access control.

Furthermore, we use IPFS as a decentralized system for storing educational certificate files. IPFS ensures the integrity and accessibility of certificate files by distributing them across a network of nodes, making them resistant to tampering or loss.

By combining the power of Hyperledger Fabric and IPFS, our system offers a robust and reliable solution for educational certificate verification. It leverages the transparency, security, and immutability of blockchain technology to streamline and enhance the verification process.

Through the implementation of these tools and components, our proposed system aims to revolutionize the way educational certificates are verified, providing a secure and efficient platform for educational institutions, employers, and individuals.

3.1. Blockchain

Blockchain technology has experienced significant development, largely driven by the emergence of digital currency Bitcoin. Blockchain refers to a distributed ledger composed of linked blocks that ensure robust security. The mechanism of the blockchain runs using a decentralised architecture, and the management of the blockchain is defined by the consensus of the members in the network. On the computer of each participant (also referred to as a node) in the blockchain network, there is a copy of the distributed ledger that is stored.

The continuous addition of blocks to the blockchain enables the storage and growth of an ever-expanding amount of data. Modifying data within the blockchain requires consensus from the majority or all of the network nodes, making it a complex and time-consuming process [10], [11].

Each new block that is added to the blockchain includes a hash of the block that came before it. This helps to ensure the integrity of the data and prevents it from being tampered with [10], [11].

Transactions are recorded within each block, and a consensus procedure is employed to verify and record these transactions. This process ensures the transparency and accuracy of the blockchain [12].

There are three categories of blockchain: public, private, and consortium. The term "public blockchain" refers to a permissionless network in its most common form (i.e., everyone can join the network, write or read, and contribute to its consensus protocol). All public blockchain networks operate without a central authority. Bitcoin and Ethereum are currently the most well-known examples of public blockchains. A permissioned network is what makes a blockchain private (i.e., only authorised users can join the network and can write or read in addition to validating transactions). Centralized systems are used by private blockchain networks. Private blockchains include the likes of Multichain and Blockstack, as two examples. The term "consortium blockchain" has also been used to refer to permission networks (i.e., only pre-defined nodes can order the transactions and add new blocks; other nodes can only send, read transactions, and verify new blocks). Two examples of blockchain networks that were established by consortiums are referred to as Corda and Hyperledger Fabric respectively [11].

By understanding the concepts of blockchain, its categories, and examples of existing blockchain networks, we can lay the foundation for implementing a decentralized architecture for educational certificate verification using the Hyperledger Fabric platform and IPFS.

3.2. Hyperledger Fabric

Blockchain technology gained significant popularity through the success of cryptocurrencies like Bitcoin. However, public blockchain platforms face challenges such as limited transaction throughput, time-consuming execution, inconsistent data, and wasted resources. To address these challenges, the Linux Foundation launched the Hyperledger project in 2015, aiming to develop a solution that would overcome these limitations [13]. Among the various blockchain platforms available, Hyperledger Fabric has emerged as the leading platform for permissioned blockchains.

Hyperledger Fabric is widely adopted in enterprise blockchain applications and is not supported by cryptocurrencies. Its network is accessible only to validated users, ensuring the security and integrity of transactions [14].

Confidentiality, resilience, flexibility, and scalability are some of the features of Hyperledger Fabric. Because of these qualities, the solution based on Hyperledger Fabric is well-suited for a wide variety of applications in the industrial sector. In order to provide this flexibility, Fabric's revolutionary architectural approach improved how the blockchain adapts to difficulties related to performance, non-determinism, and resource depletion. By utilising Hyperledger Fabric to create channels, a group of companies can create their very own transaction ledgers for their business [15].

The components that constitute Hyperledger Fabric include peers, orderers, smart contracts (chaincode), and the Fabric Certificate Authority (CA), among others. These components work together to facilitate secure and efficient transaction processing within the Hyperledger Fabric network.

By utilizing the features and components of Hyperledger Fabric, we can establish a robust and secure decentralized architecture for educational certificate verification

3.2.1. Membership Service Provider (MSP)

Hyperledger Fabric members (i.e., peers, Orderers, clients) need to register through MSP to become a part of the Hyperledger Fabric network. Accordingly, the transactions are not transparent to everyone; access permissions might be restricted to authorized members [16].

MSP provides several benefits to the Hyperledger Fabric network. It enables fine-grained control over network access, ensuring that only authenticated and authorized participants can engage in transactions. This level of control enhances the integrity and security of the network by managing membership and access permissions effectively. MSP plays a critical role in maintaining the trust and confidentiality required for secure transactions within the Hyperledger Fabric network.

3.2.2. *Peer*

Within the Hyperledger Fabric network, peer nodes are a representation of a service or piece of software that is accountable for carrying out a specific function. Peer nodes can perform a variety of tasks. They are derived from the concept of a peer-to-peer dispersed network. The peer nodes that are a part of the Hyperledger Fabric network are able to be segmented into a wide range of different categories according to the different kinds of functional activities that they carry out. The submission peer, also known as the submitter, is in charge of generating proposals and distributing them to the appropriate endorsement peer; the endorsement peer, also known as the endorser, is in charge of chaincode execution; the confirm peer, also known as the committer, is in charge of verifying the validity of chaincode execution results as well as maintaining the blockchain and ledger structure; and the final peer, also known as the confirmation peer, is in charge of maintaining the ledger structure and the blockchain itself [17]:

By utilizing different types of peer nodes, the Hyperledger Fabric network can effectively execute and validate transactions while maintaining the integrity and security of the blockchain.

3.2.3. *Orderer*

On the blockchain network, the transaction proposals that have been approved by the endorser peer nodes are arranged in the form of blocks by the ordering service. These transactions are required to receive cryptographic signatures from each endorsing peer and then be sent to the ordering service before they can be committed to the ledger. The ordering service then communicates with the committed peers on the blockchain network in order to verify and reach an agreement on the endorsement rules [18].

By orchestrating the block formation and transaction commitment process, the orderer plays an important role in maintaining integrity and consensus of the blockchain network.

3.2.4. *Channel*

In Hyperledger Fabric, organizations within the network are interconnected through channels, which facilitate private transactions between specific parties. Channels provide a means to isolate and control access to transactions and data within a defined group of participants. The introduction of channels in Hyperledger Fabric offers flexibility and scalability. Multiple channels can exist within a network, enabling separate communication pathways between different consortium entities. Each channel operates independently, allowing participants to conduct private transactions with a select group of organizations. One of the key benefits of implementing multiple channels is improved privacy. By utilizing channels, organizations can ensure that sensitive transaction information is shared only with the relevant parties, enhancing confidentiality and data protection. Additionally, channels enhance security by providing a controlled environment for participants to interact. Access to transactions and data is limited to the specific organizations involved in the channel, reducing the attack surface and potential vulnerabilities. Each channel in Hyperledger Fabric maintains its own ledger, which records the transactions specific to that channel. This channel-specific ledger ensures data isolation and transaction privacy among the participating organizations [13].

The availability of channels in Hyperledger Fabric enables a flexible and scalable approach to blockchain implementation, empowering organizations to establish private and secure communication pathways tailored to their specific needs.

3.2.5. *Client*

The term "client" refers to a set of nodes that work together to act as the final users of the blockchain network. It is the job of the client to submit a transaction proposal to endorsing peers, coordinate the outcomes of the execution, check the legitimacy of the transaction, and then send it to the ordering service when peers have validated it [19].

3.3. *Smart Contract*

Smart contracts, which are sometimes referred to as chaincode in Hyperledger Fabric, are executable distributed programmes that enable, carry out, and respect the conditions of a tamper-proof, frequently self-enforcing decentralised consensus agreement.

Transactions trigger the execution and performance of operations associated with smart contracts in accordance with the instructions that have been pre-recorded. Installed and instantiated on participants in the blockchain, they are the ones responsible for this [20].

Multiple programming languages are used to create the chaincode (e.g., Go, Java, and Node.js). Chaincode's business logic is established by members' mutual consent to read, execute, and modify the ledger's present state. Peers run chaincode to authenticate, facilitate, and enforce the rules. When a set of conditions is satisfied, the chaincode performs certain activities, and the results of the transaction execution are communicated to the blockchain network, where they are ultimately added to all the peers' copies of the ledger [21].

Smart contracts, implemented through chaincode, enable the execution and enforcement of business logic within the Hyperledger Fabric network, ensuring trust and integrity in transactional operations.

3.4. IPFS

The Inter Planetary File System, often known as IPFS, is a type of distributed file system that connects several computers that are all running the same file system. It is capable of actions that are analogous to those carried out by the BitTorrent network. It is a peer-to-peer (P2P) distributed file system that uses a distributed hash table to keep track of the locations of files and the nodes to which they are connected. The hash table that is being distributed is organized in the form of a Merkle Tree Directed Acyclic Graph table (DAG). Because of this, it is guaranteed that untrusted nodes will be unable to modify the file using the central access point. IPFS stands for Internet Protocol File System, and it is a content-address system that provides a one-of-a-kind hash to each and every file that is stored on the network. It eliminates the need for a centralized server by utilizing data deduplication technologies. IPFS will organize data that has been requested more than once so that it can be read immediately in the request that comes after it for data that has been requested more frequently. The Internet Protocol File System (IPFS) is a file system that features high performance, security, a content address storage paradigm, high storage capacity, and synchronous access [22], [23].

4. Proposed System

In the system architecture, Hyperledger Fabric is utilized as the underlying blockchain network, providing a trusted and immutable ledger for recording and managing educational certificates.

IPFS serves as the decentralized file system, ensuring secure and decentralized storage of educational credential files.

The Hyperledger Fabric certificate verification network is seen in Figure 1, and it is made up of three organizations: two peer organizations, one orderer organization, and a single channel that connects all of the organizations together.

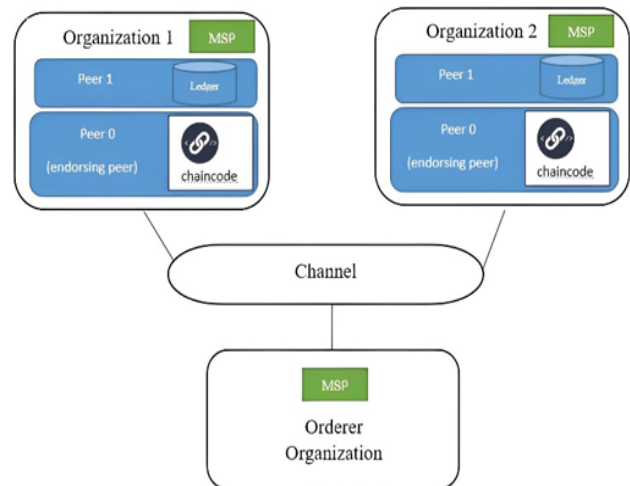


Figure 1. Visualization of the Hyperledger Fabric certificate verification network for enhanced educational credential security

Figure 1 illustrates the architecture, where organization 1 represents university A, and organization 2 represents university B. Each organization possesses its own ledger, ensuring data privacy and control over certificate issuance and verification processes.

The proposed system operates in two stages. In the first stage, certificates are issued, generated, and authenticated by the respective universities. These certificates are securely stored on the Hyperledger Fabric blockchain network, ensuring tamper-proof records.

In the second stage, the proposed system enables the verification of certificates. Using the decentralized architecture, certificate information can be retrieved from the Hyperledger Fabric network using a certificate ID. The authenticity and validity of the certificates can be verified without the need for intermediaries or centralized authorities.

By leveraging the strengths of Hyperledger Fabric and IPFS, the proposed system offers a transparent, secure, and efficient solution for educational certificate verification.

4.1. Certificate Issue Stage

The certificate issue stage is a critical component of the proposed system, focusing on the initialization and transaction flow of digital certificates for storage on the Hyperledger Fabric network.

This stage ensures the secure and reliable issuance of certificates.

Within the certificate issue stage, the process of digital certificate initialization involves several steps. These steps include the generation of certificate data, authentication procedures, and any necessary validation or verification processes to ensure the authenticity integrity of the certificates.

The transaction flow within the Hyperledger Fabric network facilitates the secure and transparent storage of certificates. This flow involves interactions between the certificate issuer, endorsing peers, and the ordering service, ensuring the proper endorsement and inclusion of certificates in the blockchain ledger.

To provide a visual representation of the certificate issue stage, an activity diagram (Figure 2) is included. This diagram illustrates the flow of activities and the interactions between the entities involved in the certificate issuance process, provide a detailed breakdown of the steps and their order.

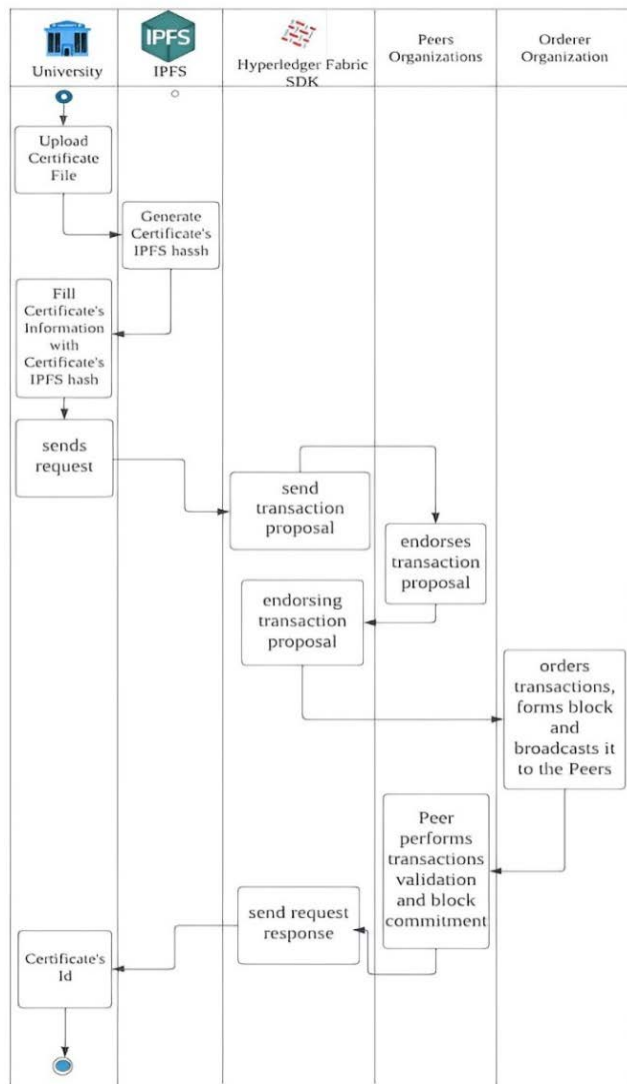


Figure 2. Activity diagram illustrating the certificate issue stage in the blockchain-based educational certificate verification system

In addition, Algorithm 1 outlines the specific steps involved in the certificate issuance process. This algorithm serves as a guide for implementing the necessary procedures, including the generation, authentication, and storage of digital certificates within the Hyperledger Fabric network.

Utilizing the transaction flow within the Hyperledger Fabric network and the processes defined in Algorithm 1, the proposed system ensures the secure and efficient issuance of educational certificates.

Algorithm 1: Certificate Issue

Inputs: certificate file, certificate information (student's full name, college, department, university order number, and university order date), and certificate's IPFS hash.

Output: the certificate's ID.

1. Upload the certificate file to IPFS to generate the certificate's IPFS hash.
2. Send a transaction proposal to execute the chaincode on the Hyperledger Fabric network, including the certificate's information and the IPFS hash.
3. Distribute the transaction proposal to all endorsing peers within each organization for endorsement and validation.
4. Send the endorsed transaction to the orderer organization.
5. The orderer initiates the transactions, forms the block, and broadcasts it to all peers in the network.
6. Peers validate transactions and add the block to the ledger after committing it.
7. Receive the response from the network, which includes the certificate's ID. Notify the university that the block has been committed on the blockchain.

4.2. Certificate Verification Stage

The certificate verification stage encompasses all procedures involved in the validation of educational certificates issued by a university. This stage is essential for assuring the validity and reliability of the certifications, establishing trust in the educational credential verification process.

Within the certificate verification stage, a series of procedures are carried out to validate the certificates. These procedures involve data retrieval, verification of certificate information, and cross-checking with the decentralized architecture comprising Hyperledger Fabric and IPFS.

To provide a visual representation of the certificate verification stage, an activity diagram (Figure 3) is included.

This diagram illustrates the flow of activities and the interactions between the entities involved in the certificate verification process, offering a clear overview of the steps and their sequence.

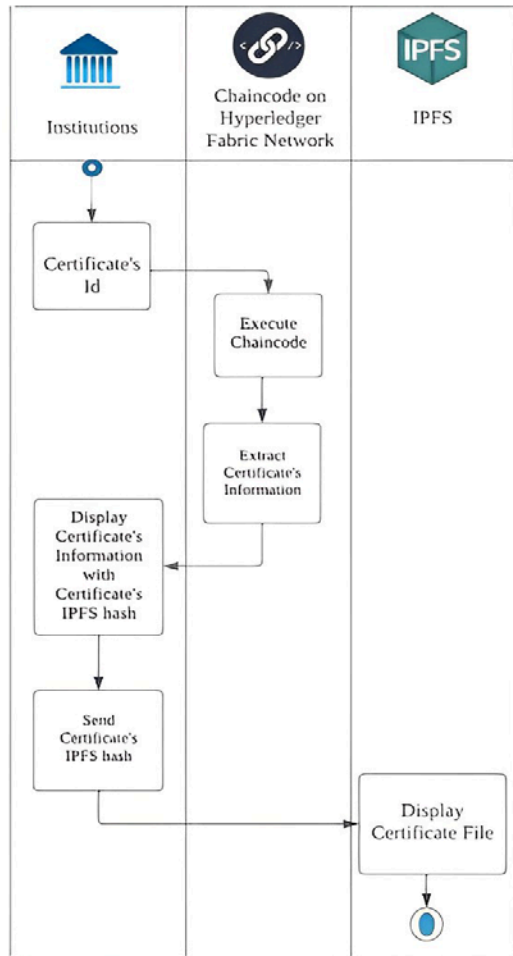


Figure 3. Activity diagram depicting the certificate verification stage in the decentralized educational certificate verification system

Algorithm 2 outlines the stages comprising the certificate verification process. This algorithm serves as a guide, providing a structured approach to validate the certificates using the decentralized architecture.

It encompasses procedures such as data retrieval, certificate information verification, and cross-referencing with the blockchain network and IPFS.

Employing the decentralized architecture and the procedures in Algorithm 2, the proposed system enables efficient and secure certificate verification, ensuring the authenticity and integrity of educational credentials.

Algorithm 2: Certificate verification

Inputs: certificate's ID.

Output: certificate's information, certificate's IPFS hash, and certificate file.

1. Submit a request to validate the certificate using the certificate's ID.
2. Execute chaincode to retrieve the certificate's information and IPFS hash from the Hyperledger Fabric network based on the certificate's ID.
3. Display the certificate's information along with the associated IPFS hash, which is stored on the Hyperledger Fabric blockchain.
4. Retrieve the certificate file from IPFS using the certificate's IPFS hash.

5. Experiments and Results

The following features of a laptop manufactured by Lenovo are utilized in the implementation of the proposed system: The CPU is an Intel Core i7-9750H @2.60 GHz, and the memory is 16 gigabytes of RAM. The operating system is Ubuntu 20.10 64-bit.

In the proposed system, Hyperledger Fabric version 2.3.2 is used. Two peer organizations (i.e. university A and university B) and one orderer organization make up the Hyperledger Fabric network. Each orderer organization and peer organization has the certificate authority (CA). By employing a single channel, the organizations are connected. The experiment results of the proposed system are shown using the Hyperledger Explorer tool. The Hyperledger Fabric network dashboard is seen in Figure 4.

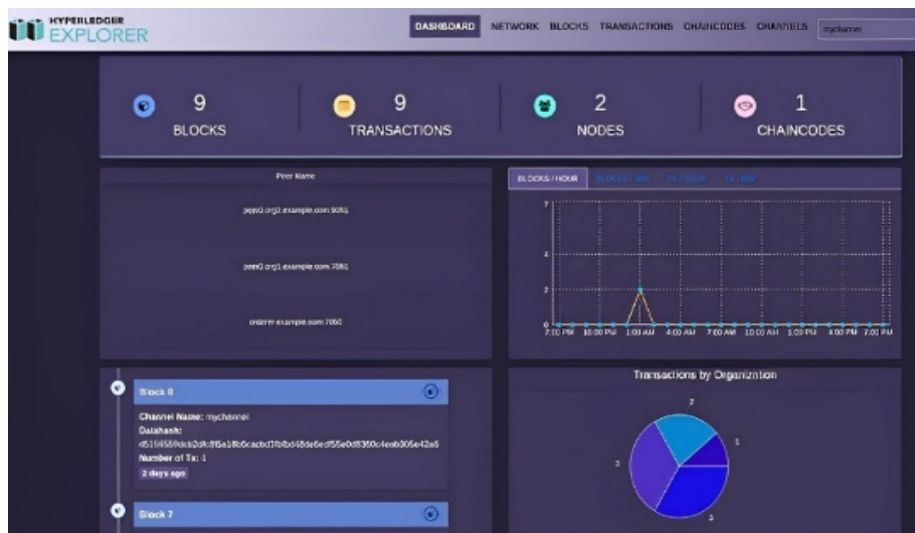


Figure 4. Dashboard of the Hyperledger Fabric network

The dashboard provides valuable information about the network, including the number of blocks, transactions, nodes, and chaincodes present in the Hyperledger Fabric network. Graphical representations depict the number of blocks and transactions produced over a certain period of time.

The circular graph illustrates the distribution of transactions conducted by organization 1 and organization 2. Figure 5 showcases the nodes or peers that comprise the Hyperledger Fabric network. It provides specific information about each node, contributing to a comprehensive understanding of the network's structure and participants.

Peer Name	Request Url	Peer Type	MSPID	Ledger Height		Unsigned
				High	Low	
peer0.org2....	peer0.org2....	PEER	Org2MSP	0	9	true
peer0.org1....	peer0.org1....	PEER	Org1MSP	0	9	true
orderer.exe...	orderer.exe...	ORDERER	OrdererMSP	-	-	-

Figure 5. Visualization of Hyperledger Fabric network's nodes and detailed information about peer entities

During the setup of the Hyperledger Fabric network and peer connections, a single channel was utilized. This channel incorporated important attributes such as the peer type, membership service provider identifier (MSPID), and ledger height, which corresponds to the number of blocks produced.

When setting up the Hyperledger Fabric network and connecting the peers, a single channel is utilized. This channel takes into account the peer type, the membership service provider identifier (MSPID), and the ledger height, which is equal to the number of blocks that are produced. Figure 6 shows a representation of the channel.

ID	Channel Name	Blocks	Transactions	Timestamp
3	mychannel	9	9	2022-04-12T22:04:33.000Z

Figure 6. Representation of the Hyperledger Fabric Network channel

Figure 7 provides a complete list of blocks and demonstrates different ways to track blocks by dates, organizations, block numbers, transactions, and channels. This facilitates efficient monitoring and retrieval of specific block information as needed.

Detailed information about individual blocks, such as the channel association, block number, creation date, number of transactions, block hash (created by the orderer organization), data hash, and reference to the preceding block (Prehash), is displayed in Figure 8.

Block Number	Channel Name	Number of Tx	Data Hash	Block Hash	Previous Hash	Transactions	Size(KB)
8	mychannel	1	d51595 ...	9e0277	f3601b ...	0e039d	8
7	mychannel	1	888d8f ...	f3601b	5f6d60 ...	ed0b0b	6

Figure 7. Comprehensive list of blocks in the Hyperledger Fabric Network

Block Details	
Channel name:	mychannel
Block Number	7
Created at	2022-04-15T22:50:26.190Z
Number of Transactions	1
Block Hash	f3601bf483fe06d56753265d4a98b41094b840831999bb24276ac07e3595dbc6
Data Hash	888d8ff8c1daee5b1908933b428bf32ee22d7aae8c93cc6a42cff7b3e8bdd48c
Prehash	5f6d6049930423829d5507d27de8e20000b79ba6acedf8b1ebb50b81b7af6535

Figure 8. Block details in the Hyperledger Fabric Network

The experiments yielded valuable insights into the proposed system. Performance metrics, including transaction throughput, verification time, and network stability, were evaluated. Results demonstrated the efficiency and reliability of the system in ensuring secure and tamper-proof verification of educational certificates.

It is important to acknowledge the limitations of the experiments. Factors such as network scale, varying transaction loads, and potential network disruptions were not extensively explored but should be considered in future research. Additionally, further analysis is required to evaluate the system's scalability, security, and resilience in real-world scenarios.

Overall, the experiments confirmed the viability and effectiveness of the proposed system, showcasing its potential to streamline the verification process of educational certificates while maintaining data integrity and security.

6. Conclusion

This paper presented an approach utilizing blockchain technology to address the challenge of educational diploma forgery.

A decentralized architecture for the verification of educational certificates was successfully designed and implemented, leveraging the Hyperledger Fabric platform and IPFS as the decentralized file system. By storing certificate files on IPFS and storing only the IPFS hash on the blockchain, the proposed system achieves immutability and reduces data storage requirements on the blockchain.

The proposed system offers several advantages. It significantly lowers the cost and effort required for verifying the authenticity of educational certificates. The lightning-fast and straightforward verification process ensures quick and reliable results.

Moreover, the system provides a robust defense against fraudulent practices, increasing trust in educational credentials.

The experimental results demonstrate the efficiency and practicality of the proposed system, overcoming the limitations of conventional certification methods. The utilization of blockchain technology, combined with IPFS, offers a secure and tamper-proof solution for educational certificate verification.

In future work, it is recommended to expand the Hyperledger Fabric network to encompass multiple organizations and implement multiple channels. This would allow for broader adoption and collaboration among educational institutions and enhance the scalability and interoperability of the system. Additionally, exploring further advancements in related technologies, such as machine learning or artificial intelligence, could enhance the capabilities and functionality of the system.

Overall, the proposed system presents a significant contribution to addressing the global challenge of educational diploma forgery. By offering a reliable and effective way for confirming educational certificates, it has the potential to change the verification process, bringing benefits to educational institutions, employers, and individuals alike.

References:

- [1]. Rasool, S., Saleem, A., Iqbal, M., Dagiuklas, T., Mumtaz, S., & ul Qayyum, Z. (2020). Docschain: Blockchain-based IoT solution for verification of degree documents. *IEEE Transactions on Computational Social Systems*, 7(3), 827-837.
- [2]. Kulkarni, D. (2021). Leveraging blockchain technology in the education sector. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(10), 4578-4583.
- [3]. Bhaskar, P., Tiwari, C. K., & Joshi, A. (2021). Blockchain in education management: present and future applications. *Interactive Technology and Smart Education*, 18(1), 1-17.
- [4]. Khan, P. W., Byun, Y. C., & Park, N. (2020). A data verification system for CCTV surveillance cameras using blockchain technology in smart cities. *Electronics*, 9(3), 484.
- [5]. Chukowry, Varshinee, Geeaneswari Nanuck, and Roopesh Kevin Sungkur. (2021). The future of continuous learning-Digital badge and microcredential system using blockchain. *Global Transitions Proceedings*, 2(2), 355-361.
- [6]. Nguyen, Binh Minh, Thanh-Chung Dao, and Ba-Lam Do. (2020). Towards a blockchain-based certificate authentication system in Vietnam. *PeerJ Computer Science*, 6, e266.
- [7]. Wang, Jian, et al. (2021). Blockchain enabled verification for cellular-connected unmanned aircraft system networking. *Future Generation Computer Systems*, 123, 233-244.
- [8]. Wang, Jin, et al. (2021). An optimized transaction verification method for trustworthy blockchain-enabled IIoT. *Ad Hoc Networks*, 119, 102526.
- [9]. Leka, Elva, and Besnik Selimi. (2021). Development and evaluation of blockchain based secure application for verification and validation of academic certificates. *Annals of Emerging Technologies in Computing (AETiC)*, 5(2) 22-36.
- [10]. Berdik, D., Otoum, S., Schmidt, N., Porter, D., & Jararweh, Y. (2021). A survey on blockchain for information systems management and security. *Information Processing & Management*, 58(1), 102397.
- [11]. Sanka, A. I., Irfan, M., Huang, I., & Cheung, R. C. (2021). A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research. *Computer communications*, 169, 179-201.
- [12]. Fernandez-Carames, T. M., & Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE access*, 8, 21091-21116.
- [13]. Iftekhhar, A., Cui, X., Tao, Q., & Zheng, C. (2021). Hyperledger fabric access control system for internet of things layer in blockchain-based applications. *Entropy*, 23(8), 1054.
- [14]. Khan, D., Jung, L. T., Hashmani, M. A., & Cheong, M. K. (2022). Empirical performance analysis of hyperledger LTS for small and medium enterprises. *Sensors*, 22(3), 915.
- [15]. Lin, J. J., Lee, Y. T., & Wu, J. L. (2021). The Effect of Thickness-Based Dynamic Matching Mechanism on a Hyperledger Fabric-Based TimeBank System. *Future Internet*, 13(3), 65.
- [16]. Lohachab, A., Garg, S., Kang, B. H., & Amin, M. B. (2021). Performance evaluation of Hyperledger Fabric-enabled framework for pervasive peer-to-peer energy trading in smart Cyber-Physical Systems. *Future Generation Computer Systems*, 118, 392-416.
- [17]. Liu, Y., Zhang, J., Wu, S., & Pathan, M. S. (2021). Research on digital copyright protection based on the hyperledger fabric blockchain network technology. *PeerJ Computer Science*, 7, e709.
- [18]. Uddin, M. (2021). Blockchain Medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry. *International Journal of Pharmaceutics*, 597, 120235.
- [19]. Surjandari, I., Yusuf, H., Laoh, E., & Maulida, R. (2021). Designing a Permissioned Blockchain Network for the Halal Industry using Hyperledger Fabric with multiple channels and the raft consensus mechanism. *Journal of Big Data*, 8(1), 1-16.
- [20]. Honar Pajooh, H., Rashid, M., Alam, F., & Demidenko, S. (2021). Hyperledger fabric blockchain for securing the edge internet of things. *Sensors*, 21(2), 359.
- [21]. Chen, C. L., Yang, J., Tsaur, W. J., Weng, W., Wu, C. M., & Wei, X. (2022). Enterprise data sharing with privacy-preserved based on hyperledger fabric blockchain in IIOT's application. *Sensors*, 22(3), 1146.

- [22]. Muwafaq, A., & Alsaad, S. N. (2021). Design scheme for copyright management system using Blockchain and IPFS. *International Journal of Computing and Digital Systems*, 10, 613-618.
- [23]. Alam, K. M., Rahman, J. A., Tasnim, A., & Akther, A. (2022). A blockchain-based land title management system for Bangladesh. *Journal of King Saud University-Computer and Information Sciences*, 34(6), 3096-3110.