2023 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN) | 979-8-3503-2284-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICPCSN58827.2023.00040

Verifcation of Academic Records using Hyperledger Fabric and IPFS

Shaik Khaleelullah
Assistant Professor
Department of Information Technology
Vignan Institute of Technology and Science
Hyderabad, India
khaleel1245@gmail.com

Sai Teja Vangapalli
UG Student
Department of Information Technology
Vignan Institute of Technology and Science
Hyderabad, India
steja065@gmail.com

Malavika Gaddam
UG Student
Department of Information Technology
Vignan Institute of Technology and Science
Hyderabad, India
malavikagoud1234@gmail.com

Vitesh Sai Hanumakonda
UG Student
Department of Information Technology
Vignan Institute of Technology and Science
Hyderabad, India
viteshvicky2001@gmail.com

Uday Kiran Goud Gangapuram
UG Student
Department of Information Technology
Vignan Institute of Technology and Science
Hyderabad, India
udaygoud2411@gmail.com

***Abstract*—Document forgery has become a significant concern recently due to the rapid development of modern technology and the simplicity of obtaining inexpensive, cutting-edge workplace supplies. Numerous cases of academic certificate fraud have been documented due to the lack of an effective anti-forgery system. Due to the lack of an effective anti-forgery system, incidents that result in the academic certificate being faked are frequently observed. As a result, methods for educational credential verification and authentication are becoming more and more necessary. Blockchain technology offers a promising solution for creating a secure, transparent, and immutable system for storing and verifying academic records. This paper proposes a permissioned blockchain-based system for verifying academic records using Hyperledger Fabric and InterPlanetary File System(IPFS). Hyperledger Fabric is a distributed ledger platform that supports smart contracts and private transactions among authorized participants. IPFS is a peer-to-peer file system that enables decentralized data storage and retrieval. The system allows academic institutions to issue digital certificates to their graduates and store them on IPFS. The hash of the certificates is then recorded on the Hyperledger Fabric blockchain. When a process is started to check if an academic certificate is real, the credentials are pulled from the off-chain database, and their hashes are generated. This hash is then compared to a hash that is already on the Blockchain. The suggested model completely satisfies all digital document verification system requirements by addressing the shortcomings and challenges in the current document verification methods.**

***Index Terms*—Blockchain, Hyperledger Fabric, InterPlanetary File System(IPFS), peer-to-peer, decentralized, smart contracts**

I. Introduction

Educational certificates are official records of a person's abilities and accomplishments in the classroom. After a person has finished a course of study or passed a test, educational organizations like schools, colleges, or universities will typically give them to them. School diplomas can be used for various things, like filing for jobs, immigration, higher education, or professional accreditation. Typical material on educational diplomas includes the school's name, the student's name, the date of issuance, the name and length of the program or course, the scores or marks attained, and any accolades or awards given. Some certificates may include extra components like signatures, stamps, or holograms to confirm the legitimacy and validity of educational certificates. Because certificates are thus valuable, people often lie about their academic qualifications by producing fake certificates.

A. *Leveraging Blockchain as the platform*

- Blockchain technology first garnered appeal as a tool to decentralize the system and eliminate intermediaries. A blockchain is a shared, distributed ledger that records transactions and is maintained by different nodes in the network who do not trust each other. Blockchain is a distributed transaction processing system with Byzantine fault tolerance [9] and untrusted nodes.
- Organizations find it helpful to connect different systems without building a centralized solution and to build trust between parties who do not trust each other or bring in a trusted third party. This blockchain property offers a secure, transparent, and immutable way to store and verify academic records. There can be many educational institutes, and all of them can issue and verify Academic records without having to trust or know other Institutes.

Satoshi Nakamoto invented Blockchain in 2008. Blockchain is one of the internet ledgers that allows for decentralized and transparent data exchange. Blockchain technology was initially used for Bitcoin in the real world. Since the coin's creation, its worth has multiplied thousands of times, primarily because blockchain technology has become so well-liked. In addition to cryptocurrencies, Blockchain is helpful for many other societal issues that result from a lack of confidence between various parties.

979-8-3503-2284-2/23/$31.00 ©2023 IEEE
DOI 10.1109/ICPCSN58827.2023.00040

Blockchain applications can operate with two types of data, namely, data saved on the Blockchain itself, referred to as on-chain data, and data stored outside of the Blockchain, referred to as off-chain data. Transactions, smart contracts, and token information are examples of on-chain data logged on the Blockchain and confirmed by network agreements. Any material not kept on the Blockchain, such as images, videos, or documents, is considered off-chain data.

On-chain data is safe, transparent, and more immutable than off-chain data because a network of nodes confirms it and cannot be changed or removed without agreement. On-chain data also guarantees interoperability and compatibility among various blockchain systems and apps. However, on-chain data have constraints like scalability problems, expensive storage prices, and privacy worries. Storing essential data on the Blockchain may decrease the network's performance and raise transaction fees. Furthermore, on-chain data is openly accessible to anyone accessing the blockchain ledger.

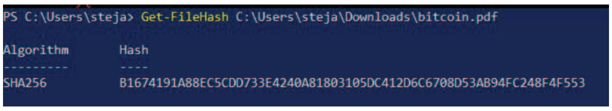
Off-chain data is any nontransactional information that is too big to be kept effectively in a blockchain or needs to be able to be altered or deleted. Off-chain data can use already-in-place services and technologies to store and handle complex or delicate data. Off-chain data also enables greater personalization and creativity in developing distinctive user encounters and features.

The Blockchain should not be used to keep nontransactional data, such as images, contracts, PDFs, and confidential information. Therefore, off-chain or database storage is necessary. Off-chain material could be more organized. The off-chain object is given a checksum or signature, which is recorded in the Blockchain.

There is an immutable checksum for Satoshi Nakamoto's Bitcoin white paper [7] of "b1674191a88ec5cdd733e4240 a81803105dc412d6c6708d53ab94fc248f4f553" (Figure-1).

This can be verified by running the below command Get-FileHash ⟨filepath⟩on Windows Powershell.

Similarly, every university degree may have an unchangeable constant hash until the data is identical. So, the storage of the hash generated from the certificate on a private blockchain has been proposed in this paper. Moreover, the credentials and the IPFS link are stored on an off-chain database. Whenever a process is initiated to verify the authenticity of an academic certificate, the stored credentials from the off-chain database are fetched, and their hash is calculated. This hash is then compared to one stored on the Blockchain for verification.



```
PS C:\Users\steja> Get-FileHash C:\Users\steja\Downloads\bitcoin.pdf

Algorithm       Hash
---------       ----
SHA256          B1674191A88EC5CDD733E4240A81803105DC412D6C6708D53AB94FC248F4F553
```

Fig. 1. Hash Code

As a result, this Blockchain would function as a lasting document repository, with all assets being decentralized and held by students and universities, respectively.

II. LITERATURE SURVEY

In 2021, A.Gayathiri, J.Jayachitra, and Dr. S.Matilda in their paper "Certificate validation using blockchain" [1] offered a blockchain-based solution to the issue of certificate forging by generating a hash of the certificate using a chaotic algorithm and stored it on a blockchain. The paper gave comprehensive information about Blockchain. It established numerous concepts about this technology, with the smart contract being the most important. The disadvantage of their approach was that the hash produced by the chaotic algorithm was image-dependent. If the picture quality is altered, the hash value will also change, which does not constitute certificate forging. The quality might vary based on characteristics like compression and watermarks and whether the picture is sent via a network.

In 2018, Rujia Li, Yifan Wu in his paper "Blockchain based academic certificate authentication system overview" [2] the author used Java and JavaScript to develop a blockchain-based certificate system. Eventually, security evaluations were undertaken from operation safety, information security, network integrity, and protocol security standpoints. The evaluation results prove that the system is sufficiently secure to fulfill corporate application requirements. The initiative is founded on the Bitcoin blockchain. The disadvantage of their method was that the upkeep of the Bitcoin Blockchain relied on tens of thousands of players in the ecosystem of cryptocurrencies. It would be irresponsible to presume that Bitcoin would continue functioning smoothly indefinitely since several stakeholders impact the blockchain ecosystem and business model.

In 2021, Priyanka Killedar, Pranav, Nachiketh S Bhat, Ravi math, and Shruthi Shetty in their paper "Blockchain based Academic Certificate Authentication System" [3] provided a concept in which a Web application was built using JavaScript, and Ethereum has the Blockchain. With the help of this paper, the capabilities of Ethereum have been learned, a public blockchain similar to Bitcoin but with more excellent capabilities. As with other public blockchains, the upkeep of the Ethereum blockchain depends on the participation of numerous ecosystem members. Furthermore, everyone is welcome to sign up and take part in the network.

In 2019, Kim-Kwang Lee, Qi Zhang, Reza M. Parizi, and Emmanuel Raymond Choo in their paper "BlockIPFS - Blockchain-Enabled Interplanetary File System for Forensic and Trusted Data Traceability" [4] proposed a notion to address the problem of file storage, This paper gave us an overview of IPFS and its potential applications in conjunction with Blockchain. The problem which was seen in the earlier paper is thus addressed. Therefore, the original document can be kept safe and retrieved whenever necessary by utilizing IPFS and Blockchain.

In 2021, Iftekher Toufique Imam, Yamin Arafat, Kazi Saeed Alam, and Shaikh Akib Shahriyar in their paper ”DOC-BLOCK: A Blockchain Based Authentication System for Digital Documents” [5] designed a system employing Ethereum and IPFS; in this system, the IPFS hash is stored alongside the certificate data, which is kept on the public Ethereum blockchain. When there is a need to access the original certificate, it can be obtained using the IPFS hash which got previously stored. In this paper, it helped us explored IPFS’s ideas and saw how it might be used to integrate IPFS with public blockchains like Ethereum.

In 2019, B. Ampel, M. Patton, and H. Chen, in their paper ”Performance Modeling of Hyperledger Sawtooth Blockchain,” [6] contrasted Fabric and Sawtooth, two members of the Hyperledger family of distributed technologies. Intel contributed to the development of a permissioned blockchain technology called Sawtooth. Hyperledger Fabric has been studied, although Sawtooth has seen far less documentation. The authors wanted to check the Blockchain’s efficiency with the help of the Hyperledger Caliper benchmarking tool so, any problems were spotted ahead of time. This paper taught us about Hyperledger Sawtooth, a private Blockchain. When comparing Fabric and Sawtooth, The Fabric community came out to be more active and to have offered helpful resources for us to employ while developing.

III. Architecture and Methodology

A. *Blockchain*

Blockchain technology, an advanced database system, permits honest data sharing across a company’s internal networks. A Blockchain database stores information in blocks linked together in a chain. Timeliness is preserved since the chain can only be broken or altered with widespread consensus. The built-in mechanisms of the system provide a consistent image of these transactions and prevent illegal transaction inputs. If assumed that the connected personal devices are nodes, Blockchain is a network of nodes linked by a Peer to Peer (P2P) communication protocol. Each node in the network must keep the data the same since all other nodes have access to the original. In addition, each node and block is encrypted using a very secure hash algorithm. In order to create a chain of interconnected blocks in the network, each block stores the hash code of the one that came before it. The resulting new hash code will invalidate the whole transaction if even a block is altered. Therefore, the decentralized structure of the network makes Blockchain a more reliable and accessible resource for storing and sharing authentic information.
In general, one block can include (Figure-2):

- Its hash value
- The hash of the preceding block
- Any information or activity that took place in that block during the procedure.

Numerous processing units spread throughout the network, numbering thousands and verifying every transaction on a block. Once the other servers have confirmed that block, it can be added to the network.

B. *Hyperledger Fabric*

To promote blockchain technologies in various sectors, the Linux Foundation launched the Hyperledger initiative in 2015. Instead of proclaiming a singular blockchain standard, it promotes an open, community-driven method for creating blockchain technologies, complete with intellectual property protections that foster open-source growth and widespread usage. One of Hyperledger’s blockchain initiatives is called Hyperledger Fabric. It is a distributed database system that facilitates smart contracts and transaction management like other blockchain-based protocols. Hyperledger Fabric is unlike other blockchain platforms in that it is permissioned and requires special access. Hyperledger Fabric networks have users join via a trustworthy Membership Service Provider instead of an open permissionless system that enables participants with unclear IDs (which would necessitate protocols like ”proof of work”) to verify transactions and protect the network. There are several extensible features available in Hyperledger Fabric. Different MSPs are allowed, various agreement methods can be switched in and out, and various forms can be used to hold ledger data.

C. *Smart Contract*

The central units of a Hyperledger Fabric blockchain are the smart contract and the distributed record. A smart contract specifies the usable logic that creates new facts added to a ledger, whereas a ledger stores facts about the current and past status of a collection of business assets. Administrators often use chain codes to simplify the implementation of linked smart contracts, which can also be used for low-level system scripting in Fabric. A smart contract specifies the usable logic that creates new facts added to a ledger, whereas a ledger stores facts about the current and past status of a collection of business assets. Administrators often use chain codes to simplify the implementation of linked smart contracts, which can also be used for low-level system scripting in Fabric.

D. *Infura*

Infura offers access to the IPFS network and Ethereum database without requiring users to manage their servers. Developers can access a flexible and dependable system through Infura, which bridges apps and the decentralized web.

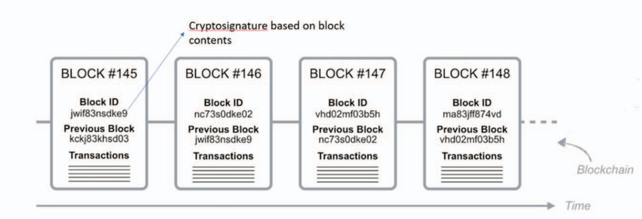


Fig. 2. Blockchain structure [13]

Users can use Infura's straightforward APIs to engage with smart contracts, make transactions, access data, and keep files on IPFS. To assist users in streamlining and ensuring the efficiency of their apps, Infura also offers monitoring, analytics, and security tools.

E. *InterPlanetary File System*

The Peer to Peer (P2P) data storage, distribution, and transmission network system is known as the InterPlanetary File System (IPFS). In order to find each file separately while connecting all computers worldwide, IPFS employs a content-based addressing scheme. Like BitTorrent, using IPFS, will give consumers access to a novel feature. Therefore, with this, a user can serve any content for other users in the network and receive content from any node with the desired content. In the IPFS system, a portion of the total data is held by specific individual administrators, offering a flexible file distribution and storage system.

F. *Hashing Function SHA256*

SHA256 is a cryptographic hash function that produces a 256-bit (32-byte) output from any input data. The original file would require significant room to store in the Blockchain. In order to uniquely map files and papers to something smaller than their initial size, a method is needed. For this, a scrambling algorithm is employed. A complicated mathematical function called a cryptographic hash function creates a unique output with a fixed length or size for every given input of varying length or size. The hash function is always one-way. Therefore, it is impossible to determine a hash function's input from its result. For digital identities and encryption, hash functions are frequently used.

G. *Architecture*

The system's architecture is divided into two parts, as illustrated in Fig. 3. The Blockchain and online application layers. While engaging with the Hyperledger Fabric network via APIs, the web application component gives users an interactive experience. The online application offers students and academic institutions a platform to share and hashing transcripts and validating transcripts. The online application uses a database of students, colleges, and other information and correlates to Hyperledger Fabric's elements. First, the register enters the details of an academic certificate into the web application. Then the application generates a unique hash representing these details through SHA 256 hashing algorithm and inserts this hash into the Blockchain. At the same time, the certificate details with the IPFS image link are inserted into an off-chain database. Then, when a verifier wishes to check the legitimacy of a certificate, the relevant information is entered into the application, which generates a hash using SHA 256 and compares it to a hash recorded in the Blockchain.

IV. Implementation

False academic records are an issue in today's educational institutions. The suggested solution calls for increased openness in the domain of certificate authentication so that all transactions or changes to records are visible to all stakeholders. Only transactions that meet specific criteria specified in the Chaincode can be committed to the Blockchain.
Due to security concerns, only college employees can change the documents; students will not have editorial rights.

A. *Hyperledger Composer*

Hyperledger Composer is an open-source, free development toolkit for building and administering blockchain apps and smart contracts on top of the Hyperledger Fabric blockchain infrastructure. It includes a collection of concepts and pre-built components, such as a domain-specific language (DSL) for defining smart contracts, a modeling language for describing business networks, and a REST API for communicating with the blockchain network to ease the development process. An illustration of the Hyperledger Composer's definitions of Assets, Participants, and Transactions is given in Table 1.
The following essential elements are used as the basis for business network design by Hyperledger Composer [8]:

- Model file (.cto): These specify network elements for the business network, including Assets, Transactions, Events, and Participants in a model file.
- Script file (.js): Transaction functions that define the business rules are described in this file. Before qualifying the Transaction entry with the organization and Asset credentials, transaction ID, and date, both of which are given by the Fabric itself, the function first determines whether the asset is qualified by determining whether the details are legitimate.
- Access Control (.acl): The permission granted to each network participant is specified in the access control file. Participants, including government representatives from different town levels, can modify and examine the information to prevent manipulation.
- Query file (.qry) : Queries are composed in a proprietary Query language.

Transactions must also have a transaction ID and a sufficient date to be valid. Hyperledger Fabric protects against the network controller having access to change those two variables, ensuring the authenticity of the created transaction.

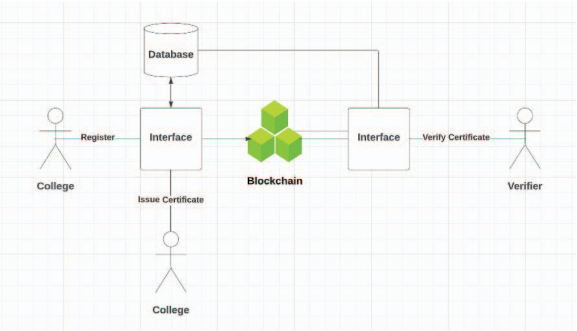


Fig. 3. System Architecture

Composer Entity	System Entity
Assets	Academic Certificates: The hash representing the Academic Certificate is generated using SHA 256 hash algorithm from the details included in a Certificate.
Participants	Central Government Educational Organizations, State Government Educational Organizations and Colleges.
Transactions	Issue of new academic certificate, updating of records.

TABLE I
DEFINITION OF COMPOSER ENTITIES. [14]

These files are bundled to create a Business Network Archive (.bna) and a .card definition distributed on the Fabric network. In Fig. 4, it is shown how assets and participants specified for the network are used to define transactions and how searching and permissions for each member work together to define the business network accurately.

Each node in a Fabric blockchain contributes to the network's overall integrity. All of the nodes in the Fabric arrangement have a unique identifier issued by a modular membership service provider due to the network's permissioned nature.

Nodes in a Fabric network take up one of three roles:

- Clients first propose transactions to be executed, then participate in the orchestration of the transactions being executed, and ultimately broadcast transactions so that transactions may be ordered.
- Peers are responsible for both the execution of transaction proposals and the validation of transactions.
- All of the peers are responsible for keeping the blockchain ledger. This data structure can only be added to and records all transactions in the form of a hash chain and the state, which is a condensed representation of the most recent state of the ledger. Only a subset of peers referred to as endorsing peers, carry out the transactions proposed by other peers. This subset's responsibility is determined by the policy of the chain code that the transaction belongs to.

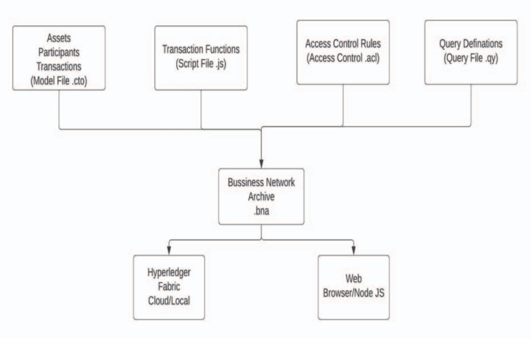


Fig. 4. Architecture of Hyperledger Composer [12]

The nodes that form the ordering service are called Ordering Service Nodes, or OSN. In essence, the ordering service is responsible for determining the overall sequence of all of the transactions that take place in Fabric. Each transaction in Fabric includes state changes and dependencies calculated during the implementation phase, in addition to the cryptographic signatures of the peers who endorse it. Orderers are entirely oblivious to the current status of the application, and orderers do not take part in either the authentication or the implementation of transactions. Because of this choice in design, the consensus in Fabric is made to be as modular as possible, making it easier to replace consensus protocols in Fabric.

Transaction Flow in Hyperledger Fabric:
Completing a transaction in Hyperledger Fabric involves many phases and several nodes, participants, and resources. The operational steps involved in a typical asset swap are outlined as follows [10].

- **Smart Contract Definition:** The smart contract, sometimes called a chaincode, is used to specify the transaction logic. The programming language in which the smart contract is written, which may be Go, Java, or Node.js, establishes the rules and conditions that must be met to carry out the transaction.
- **Transaction Initiation:** A transaction can begin with the client or the application presenting a proposal to the peers supporting it. The input data, the function that will be executed, and cryptographic signatures are all included in the proposal, which comprises all the essential information and parameters for the transaction. Endorsing peers verify the signature and execute the transaction. The peers are responsible for endorsing transactions are tasked with verifying four key elements.
  - Firstly, peers must ensure that the transaction proposal is structured correctly.
  - Secondly, peers must confirm that the transaction has not been previously submitted, thereby preventing any potential replay attacks.
  - Thirdly, peers must verify the validity of the signature by utilizing the Membership Service Provider (MSP).
  - Lastly, peers must ensure the submitter is authorized to execute the proposed operation on the channel. The inputs of the transaction proposal are utilized as arguments for the function of the invoked chaincode by the endorsing peers.
  - Proposal responses are inspected. The designated peer validates the identical proposal responses before submitting the transaction. The architectural design ensures that the endorsement policy will be verified and implemented by each peer during the validation of transactions.
- **Transaction ordering:** Using a consensus algorithm, the ordering service collects all approved transactions

and arranges them into a block. Subsequently, the block is disseminated to all the peers within the network.

- **The transaction validation and committed:** The network's peers verify the block's transactions, verify digital signatures, run smart contract codes, and examine the ledger's current status. After verifying the legitimacy of the transactions, the ledger is updated to reflect the adjustments in the situation.
- **Updating the Ledger:** Each node in the network adds a block to the growing chain of the channel, and the write sets for each successful transaction are persisted in the state database. Each node in the network will send an event to the client app after the transaction (invocation) has been verified or rejected and immutably attached to the chain.

Fig. 5 summarizes the transaction flow in detail using the swimlane sequence diagram.

Three different Colleges are operated, each with three peers and a different MSP. Every participant in the network keeps their replica of the public record.

The following is the primary functionality that the suggested prototype will have:

- After the MSP has determined that a peer is trustworthy, it will forward the suggested transaction to the ordering service.
- The ordering service will check the transaction against the accompanying chain code to ensure its legitimacy before updating the public record.
- All of the peers are notified whenever there is a change to the public ledger so that the peers can validate, approve, and update their local replica of the ledger.

Fig. 6 summarizes each distributed ledger activity that can be performed using Hyperledger Fabric.

B. *InterPlanetary File System*

Uploading and fetching files is done through Interplanetary File System. InterPlanetary File System is a peer-to-peer network aiming to accelerate, secure, and open the internet. IPFS enables users to keep and view files, websites, apps, and data without a central authority or middleman. Due to the use of content referencing in IPFS, files are recognized by their contents rather than their physical location. IPFS can prevent duplication, improve security, and maintain longevity in this manner. IPFS aims to build a distinct interconnected network, contrary to BitTorrent's decentralized approach. If two users post the same hashed piece of data, then peers receiving the material from both will receive the same data. Additionally, IPFS allows distributed hash tables (DHTs), which let users communicate with one another and share data in a decentralized way. IPFS works by splitting files into smaller chunks, hashing them, and assigning them a unique content identifier (CID). The CID is based on the file's content, not its location, so it can be used to find the file on any node.

What is a CID?

A content identifier, or CID, is a unique number that uniquely identifies a piece of material. It does not specify where data is kept but creates an address depending on the data itself. Regardless of the data's magnitude, CIDs are always short. Most IPFS material is hashed using sha2-256, so most CIDs will be the same size (256 bits, 32 bytes). CIDs are based on the content's cryptographic hash. That means:

- A new CID will be generated for any substantial changes to the content.
- When comparable data is uploaded to two IPFS nodes with the same configuration, both nodes will get the same CID.

How CIDs are created? [11]

The first step in generating a CID is to use a cryptographic technique that transforms data of indeterminate size (such as a file or data) into data of a predetermined size (such as a hash). The term ”hash” is shorthand for ”cryptographic hash digest.” CIDs store both the data's hash and its encoding method. Both

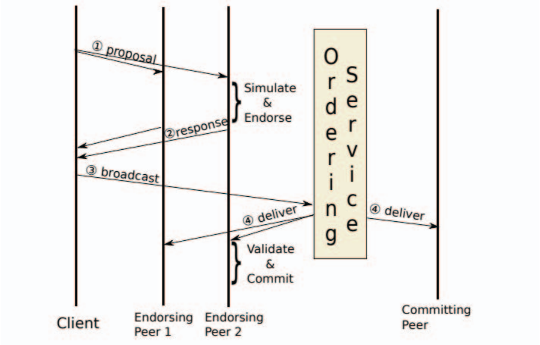


Fig. 5. Transaction Flow [10]

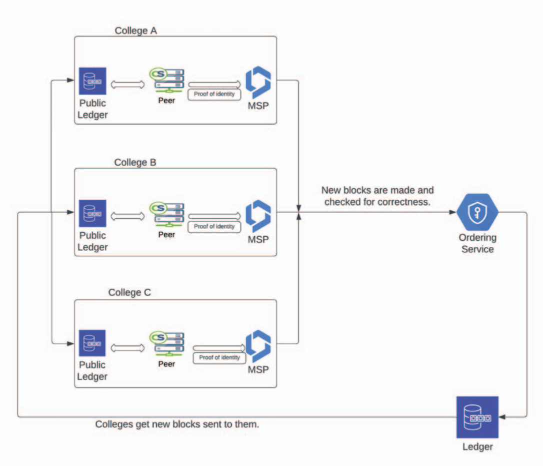


Fig. 6. Network Overview

textual and binary representations of a CID exist. The CID for a given block is often created by:

- It is computing a cryptographic hash of the data contained in the block.
- A multi-hash is a self-describing hash that includes information about the cryptographic technique used to produce it and the total length of the hash. To ensure that CIDs will continue functioning, multiformat's CIDs employ multi-hash to allow different hashing methods.

The IPFS files are pinned through Infura, as shown in Table II.

C. *Off-Chain Database*

An off-chain database is not kept in a distributed ledger. It is where digital certificates and their supporting information are kept. The off-chain database may be implemented using any conventional DBMS, such as MySQL, MongoDB, or PostgreSQL. Since the blockchain's storage capacity is limited, storing massive datasets requires the usage of an off-chain database [15]. The system efficiently manages a considerable number of digital certificates in an off-chain database, while the blockchain guarantees the immutability and security of those certificates. Certificates may be verified by comparing their hash with those recorded in the distributed ledger. The blockchain offers the required security and immutability, but the off-chain database is essential since it stores and manages digital certificates.

The MySQL database is being used to store the actual credentials of a certificate. Oracle Corporation created, disseminated, and provided assistance for MySQL, the most well-known Open Source SQL database management system. MySQL is a prevalent open-source relational database management system (RDBMS) for storing and organizing data. MySQL supports a standard form of the SQL data language, which allows us to query and manipulate data in various ways.

The college administrator enters the details into the interface, and the application calculates a unique hash representing the certificate using these details. Furthermore, this unique hash is inserted into the blockchain, which returns the Transaction ID. The Transaction ID, along with the image link, which is obtained by uploading the file into IPFS, and other details are inserted into the database.
The database is designed to store the following details:

- Time and Date of the insertion.
- Student Identity Number.
- Issuing Authority of the certificate.
- Student name.
- Certificate Identity Number.
- Certificate Name.
- The hash of the certificate generated using SHA256.
- The Transaction ID as received from the Hyperledger Fabric.
- Image link from Interplanetary File System(IPFS).

In Fig. 7, the Schema of the MySQL database is given.

Content ID's
QmfHocLvnVCG8b7UgUJM6Z2f4Q7zo8UdtFAogRgnCaPeu3
QmVihCmwcqfE98UMz3PiEDErryEDWCQszDptAoFkUPVzXW
QmeR7FbuQFT8Avdf8ehGWZH58WxCDDFMn2pSMhsHAbp5Pd
QmevSHkuuKpJheDrgQb1BqHv3udMG2gyfJNX7SSSKUooYY
QmUKahd2CABucdJhAzF1Rfen12ktpwKY2hCuP8NzZb6rD9

TABLE II
CONTENTID OF UPLOADED FILES

V. IMPROVING THE SYSTEM PERFORMANCE

The blockchain platform's performance is a significant concern for enterprise applications, and to improve the performance of the entire system, the focus should be on Hyperledger Fabric.

A. *Hyperledger Fabric*

Several characteristics, including block size, endorsement policy, channels, and a state database, are available for customization in the Fabric. Consequently, getting the values for these parameters correct is a significant obstacle to establishing a productive blockchain network. Introducing these three simple optimizations [10] can increase the overall performance of the Fabric system.

- **MSP Cache:** To save time, use a hash map with the serialized form as the key to store the deserialized identity rather than repeatedly deserializing it. Similarly, use a hash map where the key is the identity, and the value is the MSP to which it belonged, avoiding the need to verify identity repeatedly with various MSPs. In addition, use the ARC method for cache clearing and refilling. Make sure that all cached data was invalidated properly during identity revocations.
- **Parallel VSCC Validation of a Block:** VSCC serially verifies block transactions against the endorsement policy. Parallel validation, which validates many transactions' endorsements in parallel to use idle CPU and enhance speed, was researched since this strategy should have utilized more resources. On peer starting, build customizable worker threads per channel. Each worker thread verifies one transaction's endorsement signature against its endorsement policy.

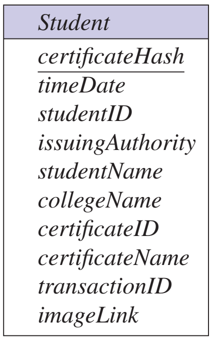

Student
certificateHash
timeDate
studentID
issuingAuthority
studentName
collegeName
certificateID
certificateName
transactionID
imageLink

Fig. 7. Schema of MySql Database

- **Bulk Read/Write During MVCC Validation and Commit:** For each transaction in a block, a GET REST API call to CouchDB via secure HTTPS obtained the latest committed version number during MVCC validation. CouchDB recommends bulk operations to reduce REST API requests. Thus, using Fabric's BatchRetrieval API to batch load multiple keys' versions and revision numbers into the cache using one GET REST API request per block.

Apart from the ways mentioned earlier, the following can also improve overall efficiency.

- **Optimizing the Smart Contracts:** Optimizing the system's smart contracts reduces execution time and improves performance. Optimizing the code and eliminating superfluous calculations will do this.
- **Caching:** Caching frequently requested data in memory reduces system response time and will speed up off-chain database access.

VI. Conclusion

This paper presented a novel Hyperledger Fabric and IPFS-based method for academic record verification. The system uses the benefits of distributed storage and blockchain technology to guarantee scholastic data's accuracy, security, and anonymity. The system allows academic institutions to issue digital certificates to their graduates and store them on IPFS. The hash of the certificates is then recorded on the Hyperledger Fabric blockchain. Any authorized entity can initiate the verification process by querying the Blockchain and retrieving the certificates from IPFS.

VII. Acknowledgement

We would like to extend our deepest gratitude to the Information Technology Department at Vignan Institute of Technology and Science, Hyderabad, for providing us with all the resources, support, and guidance needed for realizing this paper.

References

[1] Gayathiri, A. & Jayachitra, J. & Sarprasatham, Matilda. (2020). Certificate validation using blockchain. 1-4. 10.1109/ICSSS49621.2020.9201988.

[2] Rujia Li, Yifan Wu, IT Innovation Interns "Blockchain based Academic Certificate Authentication System Overview", University of Birmingham.

[3] Priyanka Killedar, Pranav L M, Nachiketh S Bhat, Ravi Math, Shruthi Shetty J. "Blockchain based Academic Certificate Authentication System", International Journal of Creative Research Thoughts (IJCRT), ISSN:2320-2882, Vol.9, Issue 7, pp.c477-c484, July 2021.

[4] E. Nyaletey, R. M. Parizi, Q. Zhang and K. -K. R. Choo, "BlockIPFS - Blockchain-Enabled Interplanetary File System for Forensic and Trusted Data Traceability," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 18-25, doi: 10.1109/Blockchain.2019.00012.

[5] Imam, Toufique & Arafat, Yamin & Alam, Kazi & Shahriyar, Shaikh. (2021). DOC-BLOCK: A Blockchain Based Authentication System for Digital Documents. 1262-1267. 10.1109/ICICV50876.2021.9388428.

[6] B. Ampel, M. Patton and H. Chen, "Performance Modeling of Hyperledger Sawtooth Blockchain," 2019 IEEE International Conference on Intelligence and Security Informatics (ISI), Shenzhen, China, 2019, pp. 59-61, doi: 10.1109/ISI.2019.8823238.

[7] Nakamoto, Satoshi. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System.

[8] Stamatellis, Charalampos, Papadopoulos, Pavlos, Pitropakis, Nikolaos, Katsikas, Sokratis, and William J. Buchanan. "A Privacy-Preserving Healthcare Framework Using Hyperledger Fabric." Sensors 20, no. 22 (2020): 6587. https://doi.org/10.3390/s20226587.

[9] M. Castro and B. Liskov. Practical byzantine fault tolerance. In Proceedings of the Third Symposium on Operating Systems Design and Implementation, OSDI '99, pages 173–186, Berkeley, CA, USA, 1999. USENIX Association

[10] Parth Thakkar, Senthil Nathan, and Balaji Vishwanathan. (2018). Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform.

[11] https://docs.ipfs.tech/concepts/content-addressing/

[12] https://hyperledger.github.io/composer/v0.19/introduction/introduction.html

[13] Why new off-chain storage is needed for blockchains. https://www.ibm.com/downloads/cas/RXOVXAPM

[14] H. Mukne, P. Pai, S. Raut and D. Ambawade, "Land Record Management using Hyperledger Fabric and IPFS," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019, pp. 1-8, doi: 10.1109/ICCCNT45670.2019.8944471.

[15] Rui P.Pinto, Bruno M.C.Silva, Pedro R.M.Inacia, "A System for the Promotion of Traceability and Ownership of Health Data Using Blockchain", 2022, DOI: 10.1109/ACCESS.2022.3203193