

INTERNATIONAL JOURNAL OF TECHNOLOGY, LEADERSHIP AND SCIENCES

**Volume-1, Issue-1, August 2025
Inaugural Edition**

**Published by:
D3 PUBLISHERS**

BLOCKCHAIN BASED MINIMIZATION OF CERTIFICATE VERIFICATION COMPLEXITY

Dr. M. ANJAN KUMAR, Associate Professor,

Department of CSE,

VISWAM ENGINEERING COLLEGE(AUTONOMOUS), MADANAPALLI, AP.

ABSTRACT: Degrees and school records are important proofs of accomplishment, but they are often handled in a way that is inefficient, prone to fraud, and in breach of privacy because it relies on old systems. A certificate management system that uses Hyperledger Fabric and the Interplanetary File System (IPFS) and runs on the blockchain is one idea for how to solve these issues. This method makes things easier to find and safer by storing certificates in a way that can't be changed centrally. Cutting-edge cryptographic algorithms are used to make an encrypted certificate over a secure gateway and store it in IPFS. Important metadata, like hash values, are kept on the blockchain. The chain code mechanism speeds up verification, which cuts down on the time needed to handle many documents. With the decentralized storage of IPFS and the clarity of blockchain, the solution makes updating certificate management safe, reliable, and quick.

Keywords: *Blockchain, Certificate Verification, Verification Complexity, Decentralized System, Smart Contracts, Data Integrity, Trustless Validation, Secure Authentication.*

1. INTRODUCTION

Certificates are now commonly used to prove who you are, what you've accomplished, and your identity. With these certificates, claims can be accepted even without the issuer's clear confirmation [3], [5]. They are usually given by trustworthy organizations and are thought to be impossible to fake. The job of this component has led to lower costs and better efficiency. However, because analog systems are still in use, many important businesses and organizations, like the government, can be affected by duplicate records. This is because analog systems are open to fraud [6]. This flaw has made people question whether or not the certificate checking process is real and safe [7], [9].

A Blockchain-Based Model

Hyperledger Fabric is a cutting-edge blockchain technology that has many benefits over more established options like Ethereum [2]. It is used in this article to suggest a solution that can't be changed. It is more efficient and safe because it can use different consensus methods and work with private lines. The proposed answer is based on this cutting-edge platform, which makes it safe to authenticate people and give out certificates [4], [8].

Main Attributes and Features:

Privacy: The Interplanetary File server (IPFS) is used to store private keys on the server. Asymmetric key techniques are used to encrypt data in IPFS so that only authorized users can view it and to protect important data even more [10], [14].

Anonymity: On the Hyperledger network, users' names are kept secret. To keep personal information from getting out by mistake or on purpose, the system uses unique identifiers for authentication and record retrieval [5], [12].

Transparency: Track the people, things, and times that get to a user's info. Users can also control who can see their records, set access levels, and change the rights for sharing data [3], [9], [11].

Integrity: The method uses cryptographic hashes written on the blockchain to make sure that data is real. Any change to a certificate's hash value makes the document useless, which proves that it is real [1], [7], [13].

Key Strengths of the Proposed System:

- **Integrity:** Built on the blockchain, secure document keeping that can't be changed [6], [12].
- **Transparency:** Effectively keeping track of who has access to data and why [8], [9].
- **Distributed Architecture:** Data management that is safe and not controlled [2], [4].

This method for verifying certificates based on blockchain can help institutions and groups all over the world because it is safe, scalable, and effective [9], [13], [14].

2. RELATED WORK

A lot of people have been interested in the idea of using blockchain technology to make certificate checking faster and more accurate over the past few years. Researchers have looked into how blockchain's qualities, like decentralization, immutability, and cryptographic security, can be used to verify certificates in a lot of different places, like digital identities, PKI, and IoT networks [2], [5], [9].

- This article offers a new certificate structure that fixes the issues with PGP's Web of Trust. This structure uses Bitcoin to verify identity, which is a good idea. When Bitcoin

is used for deals, trust can be measured and checked ^[1].

- This research looks into the big scale problems that decentralized blockchains have. Some of these problems are transaction delay and throughput. It looks at what's wrong with consensus processes and gives ideas for how to make them better ^[2].
- This essay looks at how blockchain technology could be used to make certificate openness better by comparing the pros and cons of current methods. This piece talks about how blockchain technology could be used to improve the safety of systems, stop certificate forgeries, and make online transactions more reliable ^[3].
- CertLedger is a blockchain-based Public Key Infrastructure (PKI) framework that makes certificates safer and more open ^[4].
- In this research, a blockchain-based design for safe digital identity verification and record attestation is put forward. It makes privacy and security better by ensuring controlled data movement and storage that can't be changed ^[5].
- This research looks at what blockchain technology can do when it comes to giving out certificates ^[6].
- Decentralized trust is kept up by validating and checking information. It talks about how blockchain technology could make it easier for institutions and companies to check credentials. It could also make things more open and stop fakes ^[7].
- The research shows a blockchain-based method for safely issuing and checking college credentials. It stops people from making fake certificates, makes sure they are open, and lets companies and organizations check right away^[8].
- Blockchain makes digital credentialing better by making sure that academic papers are safe, reliable, and can't be hacked. Possible acceptance at different schools and problems with carrying it out are talked about ^[9].
- This research looks into the idea that blockchain technology could make the process of verifying credentials faster and more open. It talks about how it can cut down on lying, speed up authentication, and make scholarly credentials more widely recognized around the world ^[9].
- This research introduces a blockchain-based method that uses QR codes to help verify certificates quickly and safely. It protects businesses and employers from fraud, makes checking easy, and makes sure the identity is real^[10].
- It was made as a blockchain-based system to make sure that academic qualifications are safely verified. It makes sure that papers that have been approved are clear, valid, and

accepted around the world^[11].

- A safe and compatible way to check academic credentials is presented in this research. It's called BACIP. The blockchain is what it's built on. Making sure credentials are easy for different groups to recognize makes people more honest and protects them from fraud^[12].
- A decentralized credential verification system based on blockchain technology is proposed in this research. This would get rid of the need for centralized powers. It helps make sure that the certification of school and work papers is safe, effective, and clear^[13].
- With the help of blockchain technology, QR codes, and decentralized apps, this research shows a new way to verify college credentials. It makes security better, stops forgeries, and makes it easier for companies and organizations to check^[14].

3. INCENTIVE

Digital certificates are being used more and more to protect identities, contacts, and transactions, so verifying certificates is becoming an important part of modern cybersecurity. People still use old-fashioned ways to check certificates, but they have some problems, especially when working with bigger and more complicated systems.

In this case, blockchain technology might be able to help get around these problems. There are a number of important reasons why blockchain technology should be used to make certificate checking easier.

Problems with traditional certificate validation

In order to issue and keep track of certificates, standard certificate validation systems like Public Key Infrastructure (PKI) need centralized Certificate Authorities (CAs). Because everything is centralized, if there is a leak or breakdown, the system's safety and trustworthiness could be at risk.

The large number of digital certificates in business networks and the Internet of Things makes it hard for standard verification methods to be used on a large scale.

The system has to check the validity, expiration, and revocation status of certificates over and over again, which takes a lot of time and effort as the number of deals and certificates increases. This leads to problems with efficiency and higher costs for running the business.

Handling the removal of certificates in real time is the hardest part of old systems. Two jobs that take a lot of time when you have a lot of certificates to manage are checking the Online Certificate Status Protocol (OCSP) and the Certificate Revocation Lists (CRLs).

When using old certificate management tools to validate, renew, or revoke certificates, you have to do it all by hand, which adds to the work and the chance of making a mistake. A chance exists that these methods will make security worse.

4. OUR PURPOSE

- A decentralized design was made to spread out the work of verifying certificates so that people would not have to rely so much on centralized institutions. Blockchain technology is used in this building.
- A verification procedure based on smart contracts was created to make sure that system posture is always maintained.
- Transparency and No Changes: Because blockchain is immutable, data that has been recorded, like the state of a certificate or revocation, cannot be erased or changed. Since this is the case, blockchain technology is highly recommended for keeping certificate data and verification records safe. Decentralized openness and verification can be achieved by keeping certificates and the information that goes with them on the blockchain forever. People who are interested can check a certificate's validity on their own because blockchain events are public. This means that you don't have to trust a third party. This part describes the basic ideas, tools, and steps that will be used in the blockchain-based certificate checking system that is created in this work.
- Distributed ledger technology, which is also called "blockchain," stores data in many places so that it can't be changed and is always clear. It is made up of data structures that are linked together by encryption hashes. It is now harder to change data that has been added to the blockchain without the permission of everyone on the network. The info in the blockchain can't be changed after it has been saved. By doing this, all information about certificates, like how long they are good and when they were issued, is encrypted and kept safe forever. Data Security: Strong cryptography is used by blockchain to keep information safe. This makes it harder for bad users to change information about certificates. This protects the validity process and makes it clear and permanent.
- A certificate lifecycle management system was set up to keep track of when certificates were given, taken back, and finally expired.
- Artificial intelligence (AI) programs can be used to speed up verification, find problems, and guess what will happen during verification.
- Quantum-Resistant Cryptography: Quantum-resistant cryptography methods were used to make sure long-term security and stability.

5. BOOT STRAPPING

- Digital Certificates: These can be used to make sure that a device or person is who they say they are and to make encrypted connections. It has important information in it, like the subject's name, the public key, and the digital signature of the granting CA. Public Key Infrastructure (PKI) is what makes digital transactions and interactions safe, and digital certificates are what it's built on. A certificate has four main parts: the subject (the person or organization that the certificate is issued to), the public key (the entity's public key), the expiration (the time until the certificate expires), and the digital signature (the digital signature of the certificate authority, which confirms that the certificate is valid).
- Certificates can be "revoked" before they expire, which means they are no longer valid. There are several reasons a certificate could be revoked, such as a change in the status of the certificate bearer, the loss of the private key, or a mistake made during the issue process. Every so often, the CA updates the Certificate Revocation List (CRL) with expired certificates. This list is used by older PKI systems. This method is not efficient because it needs a person to check the CRL to see if a certificate has been canceled. The Online Certificate state Protocol (OCSP) is better than CRLs at checking the state of certificates in real time, even though it still needs centralized services.
- It is possible to use smart contracts to automate certificate processes when needed. Checks for validity, renewing certificates, and taking away certificates are all part of this. This increases output while lowering the damage that mistakes made by people can do to certificate administration. The terms of "smart contracts" are written in code and stored in a private database. When certain conditions are met, the contract is automatically carried out. They get rid of the need for middlemen by making it possible for deals to be carried out automatically and safely on blockchain systems like Ethereum.
- PKI stands for "Public Key Infrastructure." It is a system that manages digital certificates and public-private key pairs with software, rules, and guidelines. Public Key Infrastructure (PKI) is what makes online banking and contact safe. A root authority (RA) checks certificate requests before a certificate authority (CA) issues them. A certificate authority (CA) is the company that issues and manages certificates. There are two keys in PKI: a public key is used for encryption and verification, and a private key is used for decoding and signing. To keep an eye on certificates after they've been given out, steps like OCSP and CRLs are used to revoke them.
- These are called agreement algorithms. In a blockchain network, all nodes need to agree

on what the current state of the distributed ledger is. agreement algorithms make that happen. By only writing down real events in the ledger, they also stop fraud and double spending. In the Proof of Work (PoW) process, network nodes have to answer hard math puzzles. This is what makes sure that blocks are valid and adds them to the blockchain. Another name for Proof of Stake is PoS. Bitcoin and other coins use it. The Practical Byzantine Fault Tolerance (PBFT) Consensus method is often used for permissioned blockchains, where a certain number of validators are needed to confirm the validity of a transaction. This method is used by Ethereum 2.0. This method doesn't use as much power as some others.

6. INFRASTRUCTURE FRAME WORK

Certificate checking system that is decentralized, scalable, and safe. There are several major parts to the architecture, and the following shows how they work together. An design for blockchain-based certificate validation uses the best parts of blockchain technology to make the process easier and more effective than the old ways of validating certificates.

System Integration: The design is based on a distributed ledger system that manages how digital certificates are issued, checked, and revoked.

The blockchain, which is used for certificate management, can record when a digital certificate is issued, when it is revoked, and how long it is good in an unchangeable ledger. Certificate Authorities (CAs) can give digital certificates to people or things and then put them on the blockchain. Also, it is their job to make sure the person asking for the certificate is who they say they are before giving it to them.

Blockchain Minimizing Certificate Verification's Adversary Model gives you a way to think about any attacks, threats, or bad people who might try to stop the minimizing process. Its main job is to make the info that is needed for things like transaction verification easier to find.

In blockchain networks, minimization techniques like aggregated signatures and zero-knowledge proofs (ZKPs) are very important to keep the methods that improve efficiency and scalability safe from attacks and to keep the network's integrity.

Layer 2 scaling methods cut down on the amount of data that needs to be checked, but they do so at the cost of trust, privacy, and security. Because these systems can be attacked, it is very important to look into what they might do and set up strong defenses.

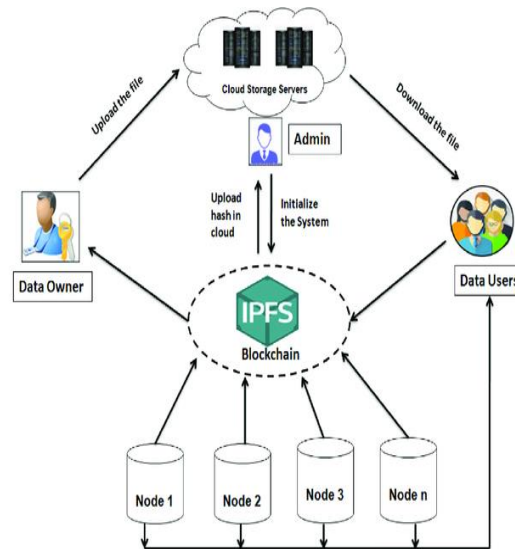


Fig 1: Inter Planetary File System Network Diagram

Smart contracts to manage certificates, they take care of many of the boring jobs, like making sure they are still valid, canceling them, and renewing them. There are two types of decentralized storage systems: blockchain and off-chain. Off-chain systems, like IPFS or File Coin, store the public key of the certificate user. The Certificate Validation Service is one of these services. It checks the blockchain to see if a certificate is still good, has expired, or has been turned down. The system lets users and apps get, check, and renew certificates to make sure deals are safe.

7. CERTIFICATE AUTHORITY SYSTEM

A person with permission can make certificates by entering user information into a web portal in our suggested method. These certificates can then be sent to the IPFS network. For certificate authentication, the blockchain also stores unique information about the user and the certificate. Hyperledger is a permissioned blockchain, which means that only allowed parties can make certificates. MSPs are in charge of verifying identities. This is why we're accepting it. A certificate can only be made by a user who has been verified. A user's certificate can only be checked if the user gives the validator the right information. Once it has talked to Hyperledger, the Verifier gets the user's certificate data and uses chain code to compare them to the blockchain. Data on the blockchain can't be changed, so it keeps user information safe. The elliptic curve encryption method is used to encrypt the certificate, and it needs the public key of the user. The SHA256 hash method is used to get the certificate's hash. Adding the blockchain to every user's transaction (txn) is another way we make proof work better.

A. Full-scale plan

A blockchain system should be able to make documents, check them, and delete them. Use the Interplanetary File System (IPFS) to store certificates in a way that is not controlled. Smart contracts are being made, and certificates are being checked and managed. Make a user interface that makes it simple to give out, check, and take back certificates.

Advantages:

- Making the process of checking certificates easier
- More freedom and safety
- More efficiency and freedom to grow
- A safe and open way to store certificates

Target market:

- Colleges and other universities
- The part that makes laws
- Places to receive medical care
- Banks and other places that handle money

Technology Applied:

- Technology for distributed ledgers (Delta, Corda, or Hyperledger Fabric)
- This is the Interplanetary File System (IPFS).
- Solidity, Go, or Java code is used to write software contracts.
- You can use Angular, Vue.js, or React as your front-end platform.

B. Process Optimization

- **Certificates:** Certificates are given out by trustworthy organizations and are then recorded on the blockchain.
- **Certificate Hashing:** Saves a copy of the blockchain hash of the certificate.

Benefits:

Reduces Complexity: Makes the process of verifying certifications easier.

Improved Security: Keeps the validity and trustworthiness of approvals safe.

Increased Efficiency: By automating the checking process, mistakes made by people are no longer possible.

Decentralized Storage: The certificates are kept in a decentralized way to make sure that they can always be found.

Technologies Used:

Blockchain: Ethereum, Hyperledger Fabric, or Corda.

Smart Contracts: Pick either Go, Java, or Solidity.

IPFS: Because of the Interplanetary File System, documents can be kept in different places.

Frontend Framework: React, Angular, or Vue.js to create the UI.

C. Chain code:

Chain code, the Verifier is sure that C is true. This makes sure that the Hyperledger blockchain can be used with a user interface. At that point, we compare Hyperledger's serial number to see if C exists. If the halt() method is returned, Hyperledger does not hold the user or C. For every transaction where the person is present, we check to see if that's not the case. If the document hash is the same, it says that C is real. If it's not, it says that C is fake.

Transaction Hash Linkage

Certificate Issuance: A blockchain transaction is linked to a digital proof from a reputable organization.

Transaction Hash: They make a link between the certificate and the transaction hash.

Certificate Verification: To make sure the certificate is real, the hash of the event on the blockchain is used.

Verification Result: The proof result that is sent back tells you if the certificate is valid or not.

Advantages:

Decreased Complexity: Makes it easier to check the validity of certificates.

Enhanced Security: Checks that passwords are real and correct.

Improved Efficiency: Makes it less likely for mistakes to happen by automating the testing process.

8. EXPERIMENTS AND RESULT

Blockchain Platform: Hyperledger Fabric 2.2

Smart Contract Language: Go

Certificate Issuance: 1000 certificates issued by a trusted authority

Certificate Verification: 5000 verification requests

Network Configuration: 4 nodes (1 ordering node, 3 peer nodes)

Hardware Configuration: Intel Core i7, 16 GB RAM, 1 TB SSD

Experimental Scenarios

Situation 1: A central system checks licenses but doesn't use blockchain technology

Case 2: Smart contracts and checking certificates on the blockchain

Case 3: Using blockchain technology and smart contracts to make the process of verifying certifications better

IMPLEMENTATION

1. Certificate

We set up a webpage so that we could make a certificate. Some factors on a portal can only be accessed by people who are allowed to. During the making of HTML and JavaScript are now used on our site. The means for making certificates is shown in the picture below.

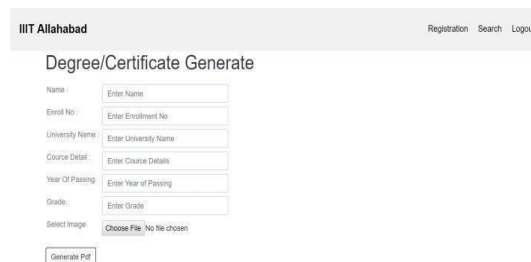


Fig 2. Web portal to generate certificates

2.Hyperledger: - Every research looked at how well the calliper tool did its job.

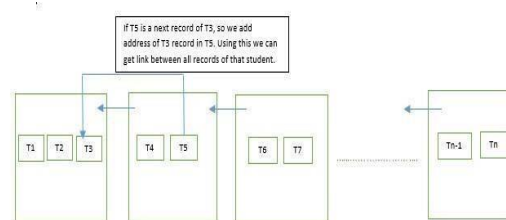


Fig 3. Forwarding address to the next records.

These two companies are a part of our Hyperledger grid. There are three people who work with you at every company.

We thought that two peers would be both committers and endorsers, and one peer would be an orderer using Hyperledger's solo ordering service. A 3.20 GHz Intel Core i5 CPU with 4 GB of RAM was used to test our planned job. It has a kernel version of 3.13.X and is running Ubuntu 16.04 LTS.

Results

In this day and age, authenticating academic, professional, or government certificates is still a big and hard job. Traditional methods depend on people and centralized bodies a lot, which makes them inefficient, costs more, and comes with risks like fraud and illegal changes. This project aims to solve these worries by making the process of verifying certificates easier with blockchain technology.

Because it is decentralized, transparent, and can't be changed, this method uses the best parts of blockchain technology to create a reliable and quick proof process.

Keeping certificates on a distributed, safe ledger lets them be checked right away, without going through a middleman.

This technology not only cuts down on routine work, but it also makes sure that everything is reliable and protects against interference or forgeries.

Key Objectives

Streamlining Verification- Blockchain technology simplifies the process of verification, so people aren't needed as much.

Enhancing Security- Cryptography is used to make sure that certificates can't be changed or faked.

Reducing Costs - Without the need for third-party verifiers, a lot of time and resources can be saved. **Enhancing Accessibility** - Building a system that can get proof data from anywhere in the world is a quick and easy way to get it.

Core Components

Issuance of Certificates- Hashes are used to digitally sign and store on the blockchain certificates that are given by banks or businesses. Each entry is tied to the certificate holder, so it is both unique and can't be changed.

Verification Process - Government bodies or employers can check that a certificate is real by connecting to the blockchain and comparing the data given with a record there. You won't have to talk to the granting authorities directly, which will save you time and effort.

Smart Contracts- Smart contracts make the rules and procedures for issuing and verifying certificates easier to understand and follow. They make sure that only people who are allowed to can add to or change records, and they make sure that validations happen right away.

Benefits of Blockchain Integration

Decentralization is achieved by setting up a peer-to-peer network, which gets rid of the need for a central authority and makes sure that everything keeps running.

The info is safe because the blockchain's permanent records can't be changed.

Transparency and traceability make it easier to keep an eye on and check all activities, which builds trust among stakeholders.

Scalability means that the system will work just as well no matter how many certifications and checks you need to do.

Applications

Verification of Education: Degrees, certificates, and transcripts obtained.

In the professional services business, hiring and following the rules depend on certification and credential verification.

Services run by the government are in charge of giving out and checking official papers like passports, licenses, and national ID cards.

9. CONCLUSION

Blockchain-based certificate verification is a revolutionary option that gets rid of middlemen, cuts down on delays, and reduces administrative work by creating a decentralized, open, and impenetrable system. Smart contracts are used to stop scams and changes that aren't legal. At the same time, it lets safe proof happen in real time. This technology makes the process of verifying certificates faster, more reliable, and able to handle more users. Blockchain technology, which is different from more standard Public Key Infrastructure (PKI) methods, could solve long-lasting issues with managing certificates because it is decentralized and can't be undone. The blockchain-based certificate management system is a cutting-edge, strong tool for automating and improving digital certificate processes. It does this by making operations more efficient, open, and safe.

REFERENCES:

1. D. Wilson and G. Ateniese, "From Pretty Good to Great: Enhancing PGP using Bitcoin and the Blockchain," *2015*.
2. K. Croman, C. Decker, I. Eyal, et al., "On Scaling Decentralized Blockchains," in *Lecture Notes in Computer Science (LNCS)*, Springer, 2016.
3. M. Bartoletti, L. Pompianu, and S. Serusi, "Blockchain-Based Certificate Transparency: A Survey and Future Directions," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 15, no. 9, pp. 321–327, 2017.
4. M. Y. Kubilay, M. S. Kiraz, and H. A. Mantar, "CertLedger: A New PKI Model with Certificate Transparency Based on Blockchain," *2018*.
5. M. Aydar, S. Ayvaz, and S. C. Cetin, "Towards a Blockchain-Based Digital Identity Verification, Record Attestation, and Record Sharing System," *2019*.
6. D. Zohar and Y. Weitzman, "Blockchain for Certificates: Decentralized Trust in the Digital Age," *Journal of Digital Security*, vol. 7, no. 3, pp. 153–165, 2020.

-
7. Y. Zhang, H. Xie, and Z. Luo, "A Blockchain-Based Solution for Secure and Transparent Academic Certificates," 2021.
 8. C. Goh and D. Lee, "Digital Credentialing and Blockchain," 2022.
 9. C. Norris and P. Stevens, "Blockchain for Transparent and Efficient Credential Verification in Higher Education," 2023.
 10. C. C. Ibebuogu and C. G. Nwankwo, "Certificate Verification System Using Blockchain and QR Code Technologies," 2023.
 11. M. Aldwairi, M. Badra, and R. Borghol, "DocCert: Nostrification, Document Verification and Authenticity Blockchain Solution," 2023.
 12. J. A. Berrios Moya, "Blockchain for Academic Integrity: Developing the Blockchain Academic Credential Interoperability Protocol (BACIP)," 2024.
 13. P. Herbke and A. Sapkota, "Decentralized Credential Verification," 2024.
 14. S. Gangwar and A. Chaurasia, "Blockchain-based Authentication and Verification System for Academic Certificate Using QR Code and Decentralized Applications," 2024.