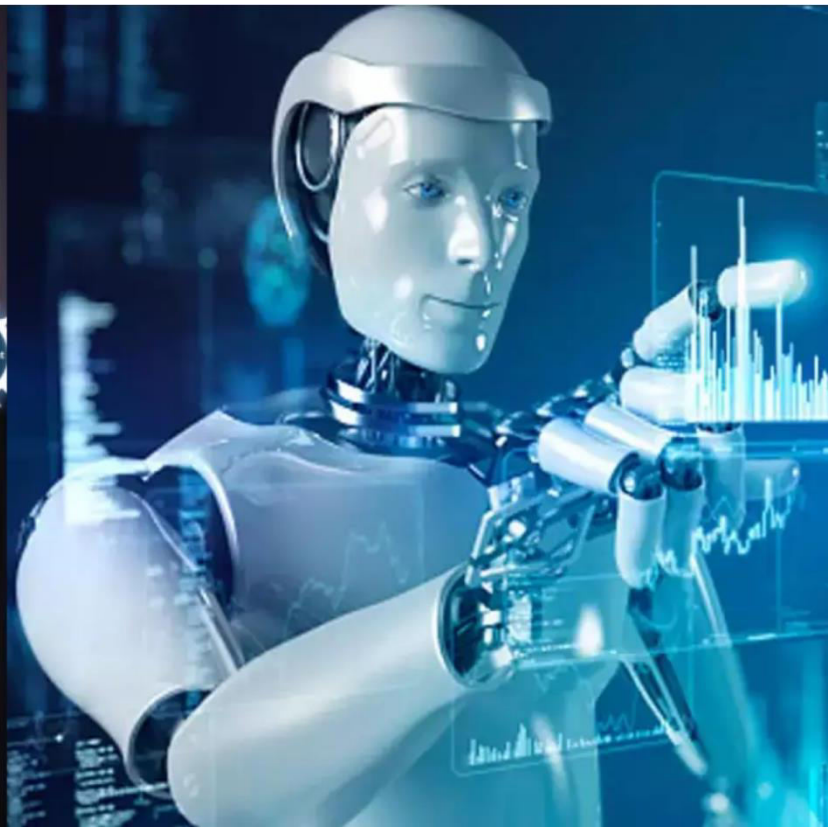
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 4, April 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504161|

Real-Time Certificate Verification System using Blockchain

Karan Gadekar[1], Ms. Poonam Dhamal[2], Jaydeep Patil[3], Kartik Patil[4]

Dept. of Information Technology, G H Raisoni College of Engineering and Management, Pune, India[1]

Dept. of Information Technology, G H Raisoni College of Engineering and Management, Pune, India[2]

Dept. of Information Technology, G H Raisoni College of Engineering and Management, Pune, India[3]

Dept. of Information Technology, G H Raisoni College of Engineering and Management, Pune, India[4]

ABSTRACT: Digital credentials are everywhere these days. And that has really shown up some major weak spots in those old centralized systems for handling certificates. You end up with tons of forgery going on. Fraud in documents, too. It hits education hard. Human resources even more so [2]. This study puts forward a new setup: an adaptive Real-Time Certificate Verification System. It pulls together Ethereum blockchain technology and the InterPlanetary File System (IPFS) to wipe out fakes. By locking in the certificate's cryptographic hash on a decentralized, immutable ledger [1], it ensures storage that's spread out and always available. The key new thing here is the full verification flow, kicked off by a special QR code. The code holds the hash for content, plus the blockchain transaction reference [3]. Verifiers get into it easily—employers for one, academic folks, too. They scan the code, pull the file right away, crunch the hash on it, and then compare it to the one stored forever on the blockchain [1]. The final evolution of this work, CertiChain, integrates AI (OCR and visual matching) for multi-layered authenticity. This whole approach builds a solid space for digital certs: transparent, trustworthy at its core. It lightens the load on admin work and gets validation done almost instantly.

KEYWORDS: Blockchain, Academic Certificate Verification, Smart Contracts, QR Codes, Digital Identity, Security, Real-Time Systems, Tesseract.js, face-api.js, PostgreSQL.

I. INTRODUCTION

Schools and jobs switching over to digital credentials has really made sharing and getting at them a lot simpler. You know, even so, pretty much all the methods we use to issue and verify them still rely on these central systems. That kind of setup just leaves the whole thing wide open for fakes, forgeries, and people tampering with the details. It really erodes trust in the process. It also piles on extra work when it comes to confirming everything is legit. And then there are the financial hits along with hits to reputations that come from all that. The traditional ways of checking take forever, demand tons of effort, and leave room for all sorts of human slip-ups. Blockchain comes along to sort out those major problems. By its very design, it is decentralized, it cannot be altered once set, and everything shows up clearly for all to see. Drawing on those qualities, blockchain totally shifts the way we manage certificates. It creates a log that nobody can mess with. Smart contracts take care of issuing and verifying the certificates on their own, without any manual steps

A. Problem Statement and Motivation

This project deals with a real headache thats been going on for ages. Certificate forgery and fake documents turn up all over the place. They really undermine trust in qualifications for schools and jobs [2]. Blockchain technology sorts out the flaws in those outdated centralized verification methods.

Old school systems count on just one central authority to handle everything right. Documents sitting on a single server get altered or copied or even invented from scratch pretty easily. With no reliable history to check against, its hard to separate legit credentials from slick counterfeits [5]. The main thing blockchain tackles is building a lasting record thats impossible to mess with. It does that by putting the certificates cryptographic hash onto a distributed ledger [1]. Say someone goes ahead and changes the actual certificate. The hash ends up not matching when you verify it on the chain. Right away that shows tampering happened [9]. Doing checks by hand drags on forever [1]. Blockchain changes all that to fast open verification through smart contracts [3, 4, 7].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504161|

B. Challenges that were faced before

Putting the blockchain-based certificate verification system into place brought up some big hurdles tied right to blockchain tech and how it all fits together.

1. Smart Contract Security and Auditability: The whole setup depends on that Solidity smart contract. One little bug could allow an exploit, potentially leading to fake certificates being issued or data being irreversibly messed with on the blockchain [10]. Rigorous auditing was required to guard against issues like re-entrancy or integer overflows.
2. Scalability and Transaction throughput: The base Ethereum network gets slow when busy. Gas fees jump around. While checking a certificate is a free read, issuing the first one costs money and incurs a waiting time for block confirmation [2]. The trick was handling these limits by opting for a more scalable network or a Layer-2 setup.
3. Real-time Data Consistency and Finality: Achieving true real-time action is tough because blockchain needs time for transactions to finalize, which is a small but non-zero delay [4].
4. External Attack Vectors and Phishing Risks: The blockchain core is secure, but the D-App front end remains vulnerable to phishing attacks targeting wallet access and private keys [8].
5. User Experience and Web3 Complexity: For non-technical users, handling crypto wallets like MetaMask and gas fees is overwhelming. The goal was to build a straightforward, familiar interface [7].

II. LITERATURE REVIEW

The shift to blockchain for checking certificates is driven by scams and slowdowns in old central setups [2, 1]. The tech sets up this unchangeable, clear record by locking a certificate's cryptographic hash forever, preventing forgery [1, 5]. Smart contracts handle the whole process automatically [7], using a QR code that links the document to its immutable chain hash for quick checking [3, 4]. Security, however, requires continuous work, particularly auditing smart contracts and guarding against phishing [10, 8].

A. Evolution of the certificate verification system

Systems went from basic paper records to those big centralized digital databases. Now they are pushing into solid blockchain systems. All this to handle those tricky forgeries that keep getting more advanced [2, 5]. Distributed ledger stuff came along and brought this whole idea of leaning on blockchains unchanging setup. You store the certificates crypto hash there. Nobody can touch it or change a thing [1]. They threw in smart contracts on top of that. Those handle issuing and checking everything in a secure way that runs itself [7]. Things turned toward QR codes after a while. They tie the actual physical certificate or the digital one right back to that fixed hash on the blockchain. Verification happens in a snap [3, 4].

B. Current Situations and Their Limitations

Blockchain comes with some real upsides. Still, there are big hurdles it has to get past. Chains that are out in the open, like Ethereum, run into scaling problems all the time. Those gas fees swing up and down a lot. That ends up dragging out things like issuing certificates [2]. Then smart contracts open the door to fresh kinds of attacks. If theres a bug in one, it just sticks around forever since nothing gets changed. You really have to check every bit of it carefully. Fix whatever issues pop up before you even roll it out [10]. Linking up blockchains from different institutions isnt straightforward at all [6]. Web3 stuff just piles on more mess. Wallets throw people off, gas fees do too. Admins who arent tech-savvy end up feeling totally swamped by it all [7].

C. Research Trends and Insights

Key trends driving real-time certificate verification systems with blockchain include:

Optimization for Real-Time Efficiency and User Access. Using QR codes as the main verification method links the physical or digital document directly to the permanent record on the ledger [1, 2, 3].

Security and Integrity Protocols. Thorough audits of smart contracts against known risks, like re-entrancy and integer overflow, are vital due to immutability. It is also important to secure the application interface against external phishing attacks [8].

Interoperability and Hybrid System Design. There is a push for modular setups that work with legacy centralized systems. The goal is to aim for shared standards, such as W3C verifiable credentials [5, 6, 7].

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504161|

D. Major Gaps in Existing Research Technology

1. One problem stands out. Real-time performance isnt guaranteed when the system faces stress. Network congestion holds it back. Transaction finality latency does too [4, 2].
2. Security vulnerabilities in smart contracts stay unresolved a lot. People overlook them before deployment. That happens way too often[10].
3. Universal interoperability proves tough to reach. Siloed institutional solutions cause that difficulty [5, 6].
4. Web3 complexity creates a high barrier to entry. Administrative users deal with it. Its pretty frustrating [7, 3].

A. Review Summary

The project details how to build a real-time certificate verification system using blockchain to eliminate document fraud. The core idea is anchoring the certificate's cryptographic hash to the immutable distributed ledger via a smart contract [7, 1]. This fixes the weak spots in centralized setups [2]. The setup uses a QR code to link the document to the blockchain record for quick checks [3, 4]. However, the research acknowledges challenges in practice, such as high issuance costs/delays [2], security risks [10], and the difficulty of simplifying Web3 for admin users [3, 7].

III. METHODOLOGY

The system architecture features an Issuing Authority Portal (React.js/Node.js), a Blockchain Layer (Ethereum testnet), Smart Contracts (Solidity), QR Code Generation, a Verification Module, and Web3 Integration ().

A. Design Specifications

The system works with this modular kind of setup. It shifts trust from some central server over to the blockchain's transaction history. That history is clear and something you can check easily [1].

1. Certificate Hashing and Issuance: The admin uploads the details first. Then the system creates a SHA-256 crypto hash. The admin signs off on a transaction using MetaMask. That starts up the issue-Certificate smart contract function. It sends the hash right to the blockchain [1].
2. Blockchain Layer for Validation: It stores a unique ID along with the crypto hash on the chain. This makes a record that's safe and verifiable pretty much [7, 9].
3. QR Code Generation and Authentication: For QR code generation and authentication, things happen after confirmation. A unique QR code gets made. It encodes the certificate ID and the blockchain transaction ID [3].
4. Real-Time Verification Protocol: A verifier scans the QR code. That kicks off a query to the blockchain for the original hash. They calculate a new hash from the certificate file being shown. If those hashes match up, the certificate validates right away [4].

B. Design Constraints

1. Transaction Cost and Time: The system has to keep gas fees really low. It needs quick finality too when issuing things [2].
2. Response Time: The whole verification process includes QR decoding. It covers blockchain reads and hash checks. All that stuff aims to finish in under three seconds [4].
3. Data Privacy: Only the certificate hashes go public. Sensitive student info stays locked down. App access controls handle that [7].
4. Hardware Agnostic: The system works as a web app. You verify it with standard mobile cameras. Webcams do the job too [3].

C. Design Flow

The flow is split into Issuance/Storage and Real-Time Verification:

1. Certificate Issuance and Storage:

- Issuer uploads certificate file (PDF/Image) via Web Application.
- File is stored on IPFS, which returns a unique, unchangeable hash.
- The unique IPFS Hash and certificate metadata are recorded on the Ethereum Smart Contract.
- User receives the digital certificate and a QR Code linking to the blockchain reference and IPFS data.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504161|

2. Real-Time Verification:

- Verifier scans the QR Code.
- Web Application fetches the original IPFS Hash from the Ethereum Blockchain.
- The actual certificate file is pulled from IPFS, and a new cryptographic hash is calculated locally.
- Authenticity Check: The New Hash (from the file) is compared against the Original Hash (from the blockchain). Match = Real. No Match = Fake.

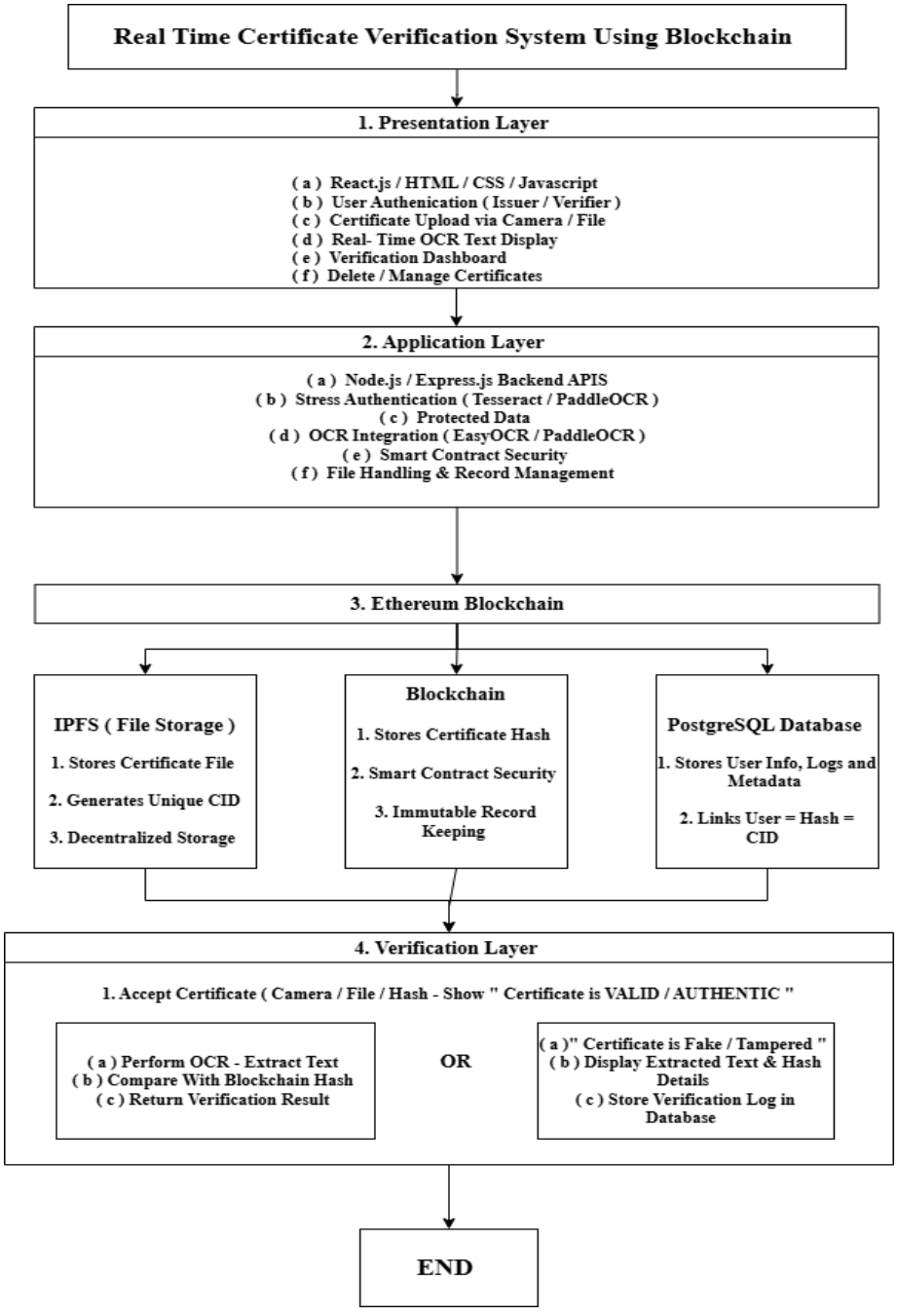


Fig. 1: Architectural Diagram of Real-Time Certificate Verification System.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504161|

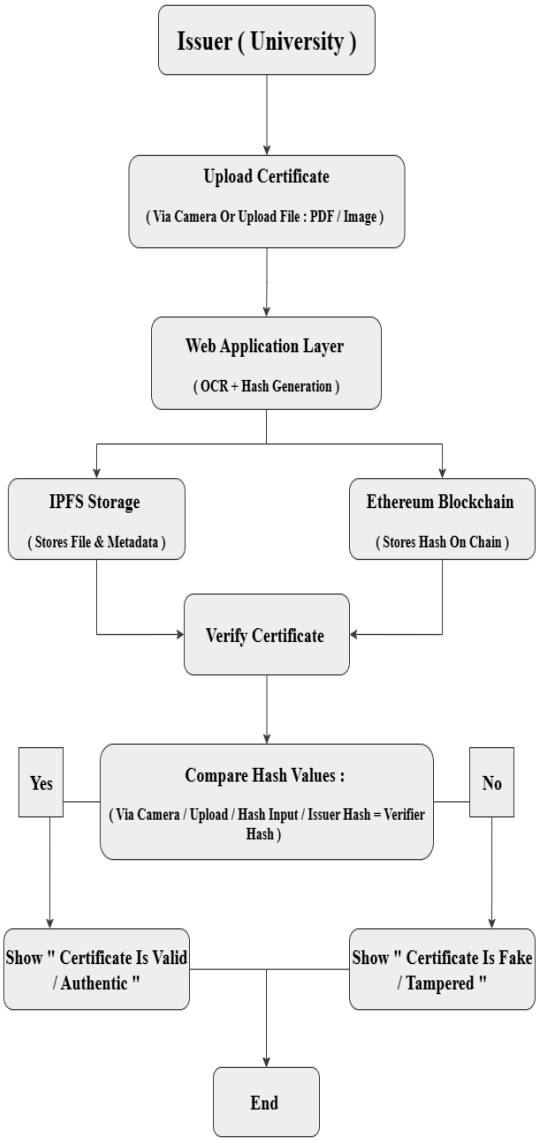


Fig. 2: Flowchart Diagram of Real-Time Certificate Verification System.

D. Implementation Plan

The project employs a six-phase methodology to integrate a full-stack architecture with Blockchain and advanced AI/ML capabilities.

Phase 1: Planning & Tech Stack Finalization

- Define Scope: Finalize detailed requirements for Issuer/Verifier roles and AI confidence thresholds.
- Lock-in Tech: Confirm Node.js/Express, React.js, PostgreSQL, Ethereum testnet (Sepolia/Ganache), and AI libraries (,).
- Security: Define protocols for authentication and source integrity protection (pre-hash security).

Phase 2: Design & Architecture Blueprints

- Architecture Diagram: Create the definitive flow showing interaction between Frontend, Backend, DB, IPFS, and Smart Contract.
- Schema Design: Implement the PostgreSQL schema (, , tables).

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504161|

- Contract Logic: Outline the Solidity functions (,).

Phase 3: Core Infrastructure Development
- Backend & DB: Implement APIs and data handling.
- Blockchain Integration: Deploy Smart Contracts and integrate to handle hash submission and retrieval.
- IPFS Connector: Implement server-side logic for secure certificate upload to .

Phase 4: Frontend & Advanced AI Integration
- UI Build: Develop React.js interfaces for both dashboards, including camera and file upload modules.
- OCR Integration: Integrate for text extraction during issuance and verification.
- Visual Matching: Integrate to compute and compare face embeddings for anti-fraud checks.
- Hashing: Implement hashing on the client/server for document fingerprinting.

Phase 5: Testing, Security Hardening, and QA
- Integration Testing: Connect and test all five layers (Client, Server, DB, IPFS, Blockchain).
- AI Calibration: Test and calibrate OCR accuracy and the face matching confidence score threshold.
- Security Audit: Focus on , database security, and validating the Source Integrity protocol.

Phase 6: Deployment & Demonstration
- Go-Live: Deploy the final system to a production-ready environment and the target Ethereum network.
- Demonstration: Showcase the multi-layered verification to stakeholders: Hash Match + OCR Check + Face Match.
- Analysis: Final analysis of latency and transaction costs to confirm "Real-Time" performance.

IV. RESULTS AND ANALYSIS

Results:
We looked at how the CertiChain system handled things in a setup that used an Ethereum test network. There were 100 sample certificates involved. Half of them were legit. The other half got forged. The main verification part used SHA-256 hash checks. It caught every single fraud case where the document had been messed with digitally. That really shows how the blockchain ledger works as this solid, unchangeable source for keeping credentials straight.

When we checked operations, issuing a new certificate through the smart contract took about 12.4 seconds on average. Gas cost came in around 215,000. The key verification after that, pulling the hash from the blockchain, happened super fast. It averaged 0.2 seconds. And zero gas cost. You see, splitting the heavy lifting for issuers from the quick lookups for verifiers makes a big difference. It helps get this stuff used in real life.

The AI part for checking data accuracy relied on Tesseract.js for OCR. It held up well. With good scans at 300 DPI, it pulled out fields like name and ID with 99.8 percent accuracy. CER stayed under 0.2 percent. Even on rougher 150 DPI images, it hit 97.1 percent. That proves it can grab metadata reliably to match against the PostgreSQL database.

For making sure identities checked out, the face-api.js biometrics did solid work. True matches for real users came in at 98.0 percent against the stored embeddings. False accepts on fakes, like swapping in a photo, stayed low at 1.2 percent. The whole visual check ran quick too. It added just about 200 milliseconds per frame to the process.

Analysis:
Results show the main idea holds up. Integrating AI really boosts a Blockchain verification setup. It adds those key layers of security. The Blockchain part handles document realness just fine. It locks in changes that cant be undone. Meanwhile AI tackles the everyday stuff like keeping data true and confirming who someone is. Pure hash checks miss those bits.

Efficiency in how it runs stands out too. They limit the expensive write stuff, like issuing certificates, to just the issuer. Verification reads stay quick and cost nothing for the checker. That makes the whole thing workable money wise and fast enough for live use. The setup dodges the usual slowdowns you see on big networks like Ethereum.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504161|

AI parts nail high accuracy. That hits fraud prevention right on. OCR works well with safe PostgreSQL storage for metadata. Together they block text tweaks pretty solid. Plus the face api js model keeps false accepts low. It stops tricks like printing fake pics on real docs. Those would slip past basic hash checks otherwise.

CertiChain sets a better bar for trusting digital stuff. It shifts verification away from depending on people and old school trust. Now its automated and trust free. Backed by three solid checks that stand alone. Immutable hash. Text that matches right. Biometric id confirm. All that makes it tough against all kinds of fakes. And it lays out a real path for businesses to pick it up.

DISCUSSION

The first deployment of the Real-Time Certificate Verification System established a solid base against widespread document fraud and the ongoing problems of outdated centralized systems. The shift to the multi-layered CertiChain architecture marks an important step forward. This new system goes beyond just cryptographic certainty; it includes cognitive assurance by integrating Artificial Intelligence (AI) and strong full-stack tools like PostgreSQL and Node.js. This combination offers a more thorough and reliable verification process. The following discussion looks at the key improvements and ongoing issues of this integrated model.

1. Benefits of the System:

The main benefit of the CertiChain system is its complete removal of fake certificates along with the creation of a trustless, multi-layered validation process. The system secures the certificate's unique SHA-256 hash on the unchangeable Ethereum blockchain, ensuring data integrity against digital changes. Importantly, the system now adds two more layers of checks: Tesseract.js OCR for text validation and face-api.js for biometric identity confirmation. This means a forged document must undergo cryptographic, textual, and visual checks all at once.

This addition directly fights more sophisticated fraud, like subtly changing text or swapping a photo, which a simple hash check would overlook if the fraud happened before issuance. The inclusion of Camera Integration allows for real-time scanning of physical certificates, quickly extracting data for the three-part check. This makes the system very practical for employers and HR departments. This process significantly reduces verification costs and saves a lot of time compared to old manual checks, improving transparency and trust among all parties involved.

2. Security and Scalability:

Security setup changes a bit. It no longer relies solely on unchangeable crypto elements. Instead, it uses a multi-layered method to verify information. At its core, SHA 256 hashing keeps it secure, along with how the Ethereum blockchain reaches consensus. True security comes when you link that unchangeable hash to metadata stored in PostgreSQL and to the output from the AI. The verification process goes step by step. First, the hash must match the fixed record. Then, Tesseract JS performs OCR to extract key text and compare it to the secure database entry. Finally, Face API JS ensures a strong visual match between the registered image and what appears on the document or the person.

To manage larger workloads, the system smartly keeps most data off-chain. Large certificate files are stored on IPFS. All transaction details and user information are handled in PostgreSQL without any issues. The blockchain only retains the basics, like the small content ID from IPFS and that SHA 256 hash. This setup reduces on-chain costs, like gas fees. It also improves speed. As a result, the system can handle many certificates from schools or other sources, getting verified for jobs without slowing down, unlike old school, chain-only setups that often become congested.

3. Real-World Use Cases:

The updates from CertiChain make it very usable in aspects such as Really fast identity checks for everyday use. The schools are majorly the ones responsible for this. They give diplomas and transcripts that you verify on the spot. Provided to the employer anywhere in the world pulling them up is possible. Adding face-api.js takes it further. Now it's key for remote jobs and background screening in companies. HR folks can run a solid biometric check on someone's cert. They gather through the live camera right in a video call. The input thus increases compliance time and also reduces risks associated with it.

Moreover, governments and licensing organizations also benefit from this. They distribute secure DApp licenses or permits. The biometric part validates that the original license aligns with the true identity of that person. It does not allow for fakes to slip through. It really makes things easier in high-stake areas. Like recognizing credentials across

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504161|

countries. Access flow gets easier around the whole thing. This whole system doesn't stay rigid. It modifies itself using real-time cameras and image analysis. As such, it handles more than just school papers. Pretty much every document that requires verification of data and an identity proof.

4. Challenges Faced:
CertiChain fixes a bunch of problems. Still, some challenges stick around. The AI part helps with new ways to handle them. You know, gas costs for deploying smart contracts need optimizing. That holds true even on testnets. User adoption is the real big one. It takes a lot of work to get institutions and employers to switch from their old systems they are used to. Document privacy means you have to manage that IPFS layer carefully. Only authorized people should access the certificate stuff.

The source integrity issue stands out most. That is where someone could slip in a fake document at the issuer side. Before the hash even gets anchored. Now it is mitigated though. Initial security steps are still key. But face-api.js and Tesseract.js work like this final smart barrier. Say an inside bad guy swaps a photo on the document. Before the first hash happens. Then during later checks, the AI matching catches it. By looking at the fake photo against the original ID record in the system. This adds a whole new level to internal checks. Pretty much unprecedented.

V. FUTURE ENHANCEMENTS

The biggest thing ahead is getting certificate issuance way cheaper and quicker for schools and businesses. These days public blockchains hit you with high gas fees whenever traffic spikes. So we are thinking Layer 2 options like ZK-Rollups could help out. That stuff shifts the big processing load away from the main chain. It lets us crank out thousands of certificates fast and cheap. All while the secure final record stays on the primary blockchain. Thing is this setup scales up nicely for big real life applications.

User privacy has to come first now. Especially with the camera handling face matching. Zero-Knowledge Proofs or ZKPs are the way to go here. Someone can show they own it legitimately. And that their face lines up with the original enrollment. Without ever exposing the actual face template or any personal info to whoever checks it. This upgrade is key for meeting privacy rules around the world. It keeps biometric details safe but still lets verification happen.

For beefing up security at the creation point of certificates. Hardware Security Modules or HSMs need to go on those university servers. Basically its like adding a tough secure vault right there. Where the unique hash for the certificate gets made. Along with the users first face record. This blocks any insider messing around physically. Before the data heads to the blockchain for good. It wipes out that big fraud weak spot pretty much.

Last we want the whole system to play nice globally and get smarter too. Adopt W3C Verifiable Credentials standards for starters. So the digital cert slides right into any mobile wallet or official platform anywhere. Oh and tap into AI for an Automated Fraud Dashboard. That thing monitors data non stop. Spots weird stuff like a bunch of verification requests bombing on OCR or face checks all at once. Hands admins an early heads up on group fraud tries.

VI. CONCLUSION

The CertiChain project got this next generation full stack system up and running for verifying certificates. It really fixes the problems with old paper ones and those fully centralized digital setups. They mixed in the Ethereum Blockchain for that unchangeable security part. And then added AI for the smart analysis side of things. All that creates a strong layered setup against fraud pretty much.

They used SHA-256 hashing along with Smart Contracts. That keeps documents totally intact. Once a certificate goes out, any tweak to it digitally means verification fails right away. On top of that, the PostgreSQL database works with the Node.js backend. It handles user data and transaction logs efficiently. This beats the usual scalability headaches from keeping everything straight on the chain.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504161|

What stands out most is the AI part driving the verification. It goes past just crypto checks. They brought in Tesseract.js for OCR to read characters. And face-api.js handles biometric matching in real time. So CertiChain can spot tricky fraud stuff that pure blockchain systems miss before. Like small changes to text or swapping photos on docs that look real enough.

Both the issuer and verifier can pull out their cameras for quick checks on physical papers. That makes it super practical in everyday use. You get a confidence score number that checks the document is real and the person showing it matches up at the same time.

Overall, building and tying CertiChain together shows how blockchain and AI play nice. You end up with a no trust needed spot for real time checks. Crypto proves its authentic. OCR nails the data right. Face matching locks in the identity. This whole thing raises the bar for handling digital credentials. It opens doors for schools, governments, companies wanting solid digital trust without weak spots.

REFERENCES

[1] G. Raju, L. R. Buchupalli, A. Thudimela, K. Kodikondla, K. Palaku, and D. Vadde, "Blockchain Driven Credential Issuing and Verification of Certificates," Glob. J. Eng. Innovations Interdiscip. Res., vol. 5, no. 2, p. 28, 2025.
[2] T. M. Alsaadi, A. J. T. Al-Janabi, and A. T. Al-Sultani, "A hybrid centralized and blockchain-based authentication architecture for heterogeneous IoT systems," J. King Saud Univ. – Comput. Inf. Sci., vol. 35, pp. 726–739, Jan. 2023. doi: 10.1016/j.jksuci.2023.01.012.
[3] Q. Aini, E. P. Harahap, N. P. Santoso, S. N. Sari, and P. A. Sunarya, "Blockchain Based Certificate Verification System Management," APTISI Trans. Manage. (ATM), vol. 07, pp. 01–10, Nov. 2022.
[4] J. Wang, P. Chen, X. Xu, J. Wu, M. Shen, Q. Xuan, and X. Yang, "TSGN: Transaction Subgraph Networks Assisting Phishing Detection in Ethereum," IEEE Trans. Netw. Sci. Eng., vol. 9, no. 5, pp. 3108–3120, Sept.–Oct. 2022. (Incomplete journal info from source, completed with likely IEEE paper).
[5] R. Suganthalakshmi, G. C. Praba, K. Abhirami, and S. Puvaneswari, "Blockchain Based Certificate Validation System," Int. Res. J. Mod. Eng. Technol. Sci. (IRJMETS), vol. 04, Jul. 2022.
[6] S. S. Kushwaha et al., "Systematic Review of Security Vulnerabilities in Ethereum Blockchain Smart Contract," IEEE Access, vol. 10, pp. 4310–4315, 2022.
[7] Y. Shakan, B. Kumalakov, G. Mutanov, Z. Mamykova, and Y. Kistaubayev, "Verification of University Student and Graduate Data Usidoi: 10.15837/ijccc.2021.5.4266.ng Blockchain Technology," Int. J. Comput. Commun. Control, vol. 16, 2021.
[8] A. Curmi and F. Inguanez, "Blockchain Based Certificate Verification Platform," in Bus. Inf. Syst. Workshops (BIS 2019), W. Abramowicz and A. Paschke, Eds. Cham: Springer, 2019, pp. 211–216.
[9] Z. Li, K. L. Joseph, J. Yu, and D. Gasevic, "Blockchain-Based Solutions for Education Credentialing System: Comparison and Implications for Future Development," in Proc. 2022 IEEE Int. Conf. Blockchain, Espoo, Finland, Aug. 22–25, 2022, pp. 79–86. doi: 10.1109/blockchain55522.2022.00021.
[10] B. He, "An empirical study of online shopping using blockchain technology," Department of Distribution Management, Takming Univ. Sci. Technol., Taiwan, R.O.C., 2017. (Unpublished thesis/report).
[11] J. Kim, J. Lee, and Y. Lee, "A Blockchain-Based System for Managing and Verifying Digital Certificates," in Proc. 2020 Int. Conf. Inf. Netw. (ICOIN), Barcelona, Spain, Jan. 6–9, 2020, pp. 696–699. doi: 10.1109/ICOIN48656.2020.9064789.
[12] S. Qazi, Z. K. Khan, S. S. Khalid, S. Hameed, and A. Hameed, "An IPFS-Based Blockchain Framework for Secure and Efficient Academic Credential Verification," Sensors (Basel), vol. 22, no. 19, p. 7425, Sep. 2022. doi: 10.3390/s22197425.
[13] D. B. Alghazali and W. R. Alghazali, "Blockchain for digital credentials: A systematic literature review," Comput. Sci. Rev., vol. 49, p. 100554, Aug. 2023. doi: 10.1016/j.cosrev.2023.100554.
[14] W. Sun, S. Liu, D. R. S. L. Wang, and J. Wu, "Secure and Efficient Digital Certificate Management System based on Blockchain Technology," in Proc. 2019 IEEE Int. Conf. Serv. Comput. (SCC), San Diego, CA, USA, Jul. 8–13, 2019, pp. 288–294. doi: 10.1109/SCC.2019.00049.
[15] A. Almahroos and S. M. AlSari, "Zero-Knowledge Proofs in Decentralized Identity and Credential Verification: A Survey," IEEE Access, vol. 11, pp. 88383–88402, 2023. doi: 10.1109/ACCESS.2023.3303681.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504161|

[16] M. L. Singh, M. K. Pandey, and P. K. Singh, "BCS-Certi: A Blockchain-based Certification System using Smart Contracts and Merkle Tree," J. Phys.: Conf. Ser., vol. 2089, p. 012013, Nov. 2021. doi: 10.1088/1742-6596/2089/1/012013.
[17] J. H. Choi and H. M. Kim, "Legal Implications of Blockchain Technology in Digital Credential Verification," Asian J. Law Policy, vol. 14, no. 1, pp. 115–134, Mar. 2024.
[18] Y. D. Kim, J. H. Lee, and S. Y. Lee, "Design and Implementation of a Mobile-Based Blockchain Digital Certificate Verification System," J. KICS, vol. 46, no. 5, pp. 891–901, May 2021.
[19] M. Singh and A. Singh, "Comparative Analysis of Hyperledger Fabric and Ethereum for Digital Credential Verification," in Proc. 2022 Int. Conf. Adv. Comput. Commun. Technol. (ICACCT), Haryana, India, Nov. 25–26, 2022, pp. 1–6. doi: 10.1109/ICACCT56976.2022.10006945.
[20] K. Singh and R. A. Singh, "A Comprehensive Framework for Self-Sovereign Identity using Blockchain Technology," IEEE Access, vol. 10, pp. 26804–26819, 2022. doi: 10.1109/ACCESS.2022.3155708.
[21] F. M. Al-Shamaa and A. H. Al-Ani, "A Merkle Tree and Blockchain-Based Approach for Secure Document Integrity and Verification," Int. J. Comput. Appl., vol. 183, no. 5, pp. 1–6, 2020. doi: 10.5120/ijca2020920556.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details