INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING &TECHNOLOGY (IJCET)

ISSN Print: 0976-6367
ISSN Online: 0976-6375

PUBLISHED BY

IAEME

IAEME Publication
Chennai, India
https://iaeme.com/Home/journal/IJCET

International Journal of Computer Engineering and Technology (IJCET)
Volume 16, Issue 2, March-April 2025, pp. 498-515, Article ID: IJCET_16_02_033
Available online at https://iaeme.com/Home/issue/IJCET?Volume=16&Issue=2
ISSN Print: 0976-6367; ISSN Online: 0976-6375; Journal ID: 5751-5249
Impact Factor (2025): 18.59 (Based on Google Scholar Citation)
DOI: https://doi.org/10.34218/IJCET_16_02_033

ARCHITECTURE FOR A BLOCKCHAIN-BASED CERTIFICATION PLATFORM FOR EXPLOSION-PROOF DEVICES

Sukruthi Reddy Sangannagari

Senior Quality Assurance Specialist and Full Stack Developer, Fm Global, USA.

ABSTRACT

Explosion-proof apparatus is a must in hazardous areas especially in an industrial setting where certification is required to meet certain safety levels. Conventional certification mechanisms tend to be slow, non-transparent and vulnerable to forgery of documents and delays, particularly in the context of cross border transactions. This article presents the architecture of a blockchain-based certification platform, which could contribute to transparency, traceability, and efficiency in the certification lifecycle of explosion-proof equipment. It includes Ethereum smart contracts, IPFS (InterPlanetary File System) to store the comprehensive test reports on a decentralized platform, and a role-based web application interface for different kinds of users such as manufacturers, testing labs, certification bodies, and field auditors. Smart contracts are responsible for generating, revoking and handling certificate access control, all certification metadata and file hashes are suitably safeguarded on the blockchain, allowing records to remain tamper-proof and verifiable. A working prototype was implemented in Goerli Ethereum testnet and developed as React application. js frontend, Web3. js, IPFS and

MetaMask for identity control. Performance testing indicated an average certificate issuance time of 4.8 seconds, verification time of less than 2 seconds, and transaction fee of 0.0004 ETH per operation. As opposed to traditional flows, which take 2–4 weeks to certify, the proposed platform achieves certification in less than a day with full traceability and instant global verification. This paper shows that blockchain technology can help to modernize certification system of industrial safety equipment, providing a secure and scalable solution for traditional certification, and has large potential for future industrial safety application.

Keywords: Blockchain, Certification, Explosion-Proof Equipments, Smart Contracts, IECEx, ATEX, IPFS, Industrial Safety, Traceability, Compliance.

Cite this Article: Sukruthi Reddy Sangannagari. (2025). Architecture for a Blockchain-based Certification Platform for Explosion-Proof Devices. *International Journal of Computer Engineering and Technology (IJCET)*, 16(2), 498-515.
DOI: https://doi.org/10.34218/IJCET_16_02_033

1. Introduction

In hazardous ESSLE-industrial facilities such as oil refineries, chemical plants, mining facilities or gas supply systems an explosion hazard can exist from flammable gases, vapours or dust. Equipment destined for those environments — widely known as explosion-proof or Ex devices — are subject to extensive testing and certification to establish that they meet national and international safety standards such as ATEX (ATmosphères EXplosibles) in the European Union and IECEx (International Electrotechnical Commission System for Certification to Standards Relating to Equipment for Use in Explosive Atmospheres) around the world.

The construction materials that comprise explosion proof equipment can be the difference in an accident waiting to happen and workers and the rest of the public remaining out of harms way, and the protection of the condition of industrial infrastructures. The certification of these procedures is usually performed by certification agencies, notified bodies, manufacturers, and regulatory administrators. Yet, despite the urgency and official structures in place, the certification landscape suffers from a number of long-standing issues – including, among others, cumbersome paper-based handling and delay in document processing, vulnerability to fraud and fakery, and lack of real-time traceability [1].

Conventional certification processes tend to be isolated and reliant on manual handling, paper-based evidence and centralised data stores. These natures add bottleneck and difficult for the product identification parties to have the interoperable coordination, or to verify, or to audit the application certifications more efficiently. Additionally, fake certifications and non-conforming products can penetrate into the supply chains especially in areas where regulation enforcement is weak or fragmented. Security holes are not only a threat to safety but egregious trust failures in the certification system as well [2].

Meanwhile, with digital technologies coming to the fore, it's an opportunity to reform old-school certification regimes. Blockchain is an emerging technology that is potentially transformative, particularly in terms of addressing the problems associated with transparency, immutability, decentralization, and trust. With blockchain, investigators can record forever certification data on a transparent blockchain, which cannot be tampered with, and accessible to all relevant parties instantly. Smart contracts, which are self-enforcing code running on the blockchain, can govern rules and automate certification workflows, such as issuance, revocation, and verification of certificates. Moreover, DLT can be combined with other components such as IPFS for storage of big documents like testing reports, design specifications and audit trails in more efficient way than stuffing the blockchain [3].

That is not new, the potential of blockchain in certification has already been identified in areas as diverse as the management of food safety, pharmaceuticals, education and supply chains for example. IBM's Food Trust, for example, follows produce from farm to shelf, improving food traceability. Blockchain is starting to be used by universities and credentialing organizations to make tamper-proof diplomas and other educational certificates. Nevertheless, very limited studies have addressed how to apply blockchain into the context of industrial safety certification, especially for explosion-proof devices, even though it is highly related and urgent.

This paper suggests the holistic system architecture of the blockchain based certification platform which can meet the requirements of Ex equipment. The aim is to combine conventional safety certification approaches with modern, digital technologies and develop an open system, which is transparent, secure and interoperable with safety standards worldwide.

The architecture is designed to accommodate the needs of a diverse set of stakeholders, including:

- **Manufacturers**, who submit devices for certification and must demonstrate compliance.
- **Testing Laboratories** (e.g., Notified Bodies), responsible for verifying device safety under ATEX or IECEx guidelines.
- **Certification Authorities**, who issue, validate, or revoke certificates.
- **Regulatory Agencies**, who audit and oversee compliance at a national or international level,
- **End-users** and **inspectors**, who rely on valid certification to ensure the safety of deployed devices,.

The proposed block-chain platform contains quite a few key elements. It is shown in figure 1

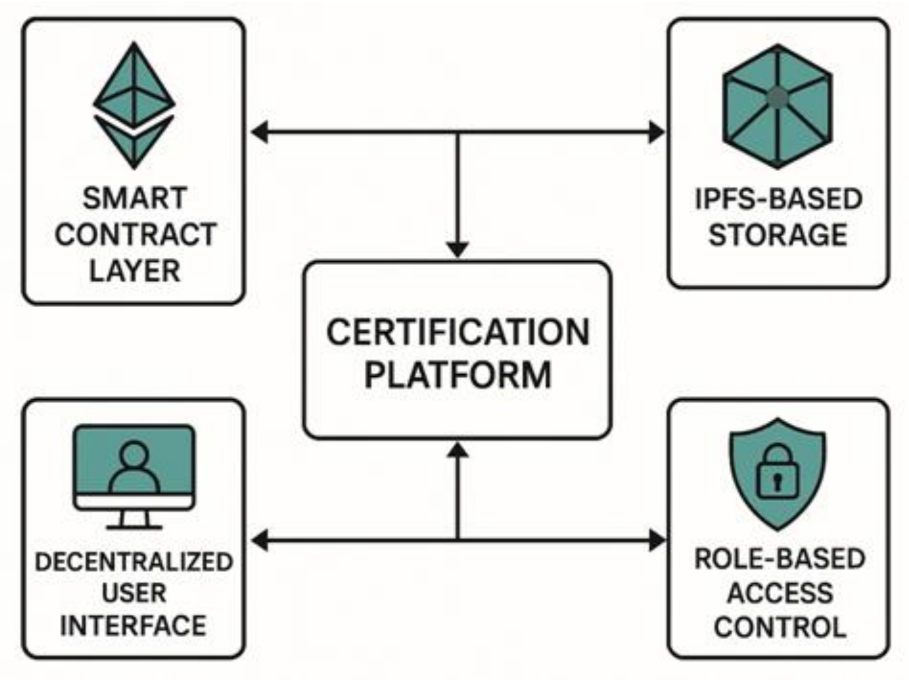

Figure 1: Architecture of the Blockchain-based Certification Platform

- A smart contract layer that embeds certification logic, access control and compliance rules.
- A Storage Layer on IPFS for an off-chain storage solution for documents and reports that is too large.
- A client-independent submission, verification, and audit interface.

- Access control mechanism (based on the user's role) to allow only authorized parties to execute sensitive operations (ie: issue or revoke a certification).

Aside from the functional aspects, the platform has been developed focusing on security, scalability, and compliance. Device test reports for instance are hashed, and the integrity is stored on-chain and the document itself stored in decentralized storage. Certificates are signed virtually using cryptographic keys associated with the issuer so that they cannot be tampered or forged. In addition, the design of the system enables an auditable trail that regulators can follow to see the lifecycle of any device or certificate — from issuance to decommissioning.

This blockchain solution can also provide better compatibility with international certification standards. In most cases, an IECEx certified product may still contrastingly need to be recognized within country-specific programs such as CSA (Canada) or ATEX. Common blockchain platform for global certification authorities to see & build on each other's immutable records without duplicates; harmonize on the compliance and accelerate speed to market of safe devices [4].

To prove the feasibility of the proposed architecture, a prototype was constructed using Ethereum to execute smart contracts and IPFS for storage of data. The prototype was evaluated in a simulated environment, which included all the major actors. Initial results indicate that certificate issuance time, human error and security are all greatly improved with cryptographic validation. Additionally, the implementation demonstrated potential areas for future optimization: integration with identity verification systems (e.g., SSI, KYC/AML), scalability improvements through Layer 2 solutions, and adoption of privacy-preserving techniques (e.g., zero-knowledge proofs) for confidential regulatory data.

In conclusion, the architecture presented has the intention to give a new meaning to how explosion-proof device certifications are administrated, emitted and consumed. With trust built into the certification infrastructure directly through the blockchain concept, it is believed the platform will ensure faster processing, more transparency, and better protection against fraud than possible with existing systems. The value lies in its ability to improve safety, compliance and operational efficiencies in some of the world's most risk adverse industries, although the concept is based on blockchain LPWAN is the critical enabler.

2. Related Work

Explosion proof devices are an essential requirement in applications such as oil and gas, petrochemicals, power generation and mining among others where hazardous atmospheric conditions can exist. Certifying these equipment creates trust in public safety standards, but it is also traditional and inefficient due to lack of transparency and potential for fraud during certification process. It is one of the valuable solution to such kind of challenges and the blockchain technology is come with decentralization, immutability, and transparency which address some of this problem. This paper reviews recent progresses on the block-chain architectural developments with respect to the certification procedures applicable to explosion-proofed devices and processes in industrial environments.

2.1 Blockchains for Industrial Certification Architectures

Liang et al. [1] proposed blockchain architecture for the supervision of the safety of special equipment. Their solution, incorporating smart contracts, will automate the certification process, resulting in the highest level of data validity and traceability in equipment certification processes. This is a resolution to the desire for an unforgivable and verifiable certification system.

Ghovanlooy Ghajar et al. [2] invented “Schloss”, a blockchain architecture for secure Industrial IoT (IIoT) environment. Using Ethereum blockchain and adaptive trust management, Schloss guarantees the secure exchange of sensing data as well as the secure device identification, which is essential for the authoring of explosion-proof devices.

Yang et al. [3] proposed a trusted-computing-hardware-based secure blockchain platform for IIoT. Their architecture also uses Trusted Execution Environments (TEEs) and specific security chips for protecting the blockchain from a range of attacks. The throughputs and confirm delay of the platform are high and low respectively, providing the practical possibility of the existence of the platform in IIoTs.

Rathee et al. [4]have developed a blockchain-enabled trust management model which can be employed to tackle security threats in IIoT networks. Their solution chooses one IoT device as the coordinator to calculate the trust of nodes, which avoids the malicious entities to take part in the network. This improves the dependability of certification mechanisms in industrial environments. Xu et al. [5] proposed BlendMAS, a smart public safety oriented, blockchain-based decentralized microservices architecture. By combining blockchain with microservices, BlendMAS enables scalable and secure data sharing for safety certification.

2.2 Enhancing Data Integrity and Traceability

Suhail et al. [6] conducted a study on the blockchain-supported digital twins, focused on industrial applications. They emphasized the ability of digital twins to support the certification and monitoring of industrial equipments and also guarantee integrity of data for predictive maintenance.

Zhou [7] developed a sensor node system in industrial internet using blockchain. The design favors data security and data management in industrial application, in particular, ensuring that the sensor data that have been used in certification process are not tampered with and that are certifiable.

Zhang et al. [8] studied a blockchain-based solution for full life cycle information traceability of industrial goods. Their design facilitates comprehensive tracking and certification along the entire lifecycle of the product, thus ensuring that explosion-protected devices remain compliant from production to phased decommissioning.

Li et al. [9] proposed a powerful blockchain framework to handle quick certification of manufactured data. Their solution is a modular and scalable system that can be adapted to existing industrial environment and supports secure certification processes that improve integrity of manufacturing data.

2.3 Secure Authentication and Access Control

Authentication is the first line of defense for any secure access control mechanism and it not only ensures the verification of a user's identity, but it also, makes users liable to any misuse of the system (e.g., sharing their password or inadvertently receiving confidential files that they do not have the appropriate privilege to access).

Shen et al. [10] put forward a blockchain aided secure device authentication for cross domain IIoT. Their solution enhances authentication that is important to certify devices to interdomain and guarantee that only the legitimate devices join industrial networks.

Li et al. [11] presented the blockchain based authentication for iIOT devices with PUF. This approach enables a better device authentication; because it provides a secure certification in IIoT networks that ensures each device holds a unique and tamper-proof identity.

Sharma et al. [12], the authors introduced the secure authentication and privacy-preserving blockchain framework for IIoT. They proved how the combination of advanced cryptography, such as zero knowledge proofs, and decentralized identity management, can guarantee data privacy and integrity, both directly impacting the trust of certification processes.

Saha et al. [13] introduced DHACS, a decentralized hybrid access control system for IIoT, based on smart contract. Their model enhances current access control mechanisms to enable a secure management of certification, where only certified parties can obtain and change certification data.

Cui et al. et al [14] developed an outsourcingsupported anonymous multi-authority access control scheme for edge-based IIoT systems. Their method increases privacy and access control meaning that it can be used for decentralized certification since it employs many authorities that attribute access rights but not user identity.

Zhang et al. [15] surveyed blockchain based decentralized trust management in IoT. Finally, the driving factors, challenges and solutions for trust management, which is a critical requirement for certification in IoT systems, have been introduced by utilising blockchain to facilitate trust among distributed entities.

The development of blockchain system for the certification of explosion proof devices demonstrates the advances in the trust, transparency and efficiency of the certification process. The surveyed literature presenting architectural solutions we noted diverse design strategies such as smart contracts, trusted computing hardware, digital twins, or enhanced access control systems. Together, these advances combine to offer more robust & efficient certification processes that help to establish confidence that explosion-proof products will conform to safety requirements during every stage of their existence.

3. Proposed Architecture

The proposed architecture of a Blockchain-based Certification Platform for Explosion-Proof Devices is illustrated in Figure 2. It is made up of following major components:

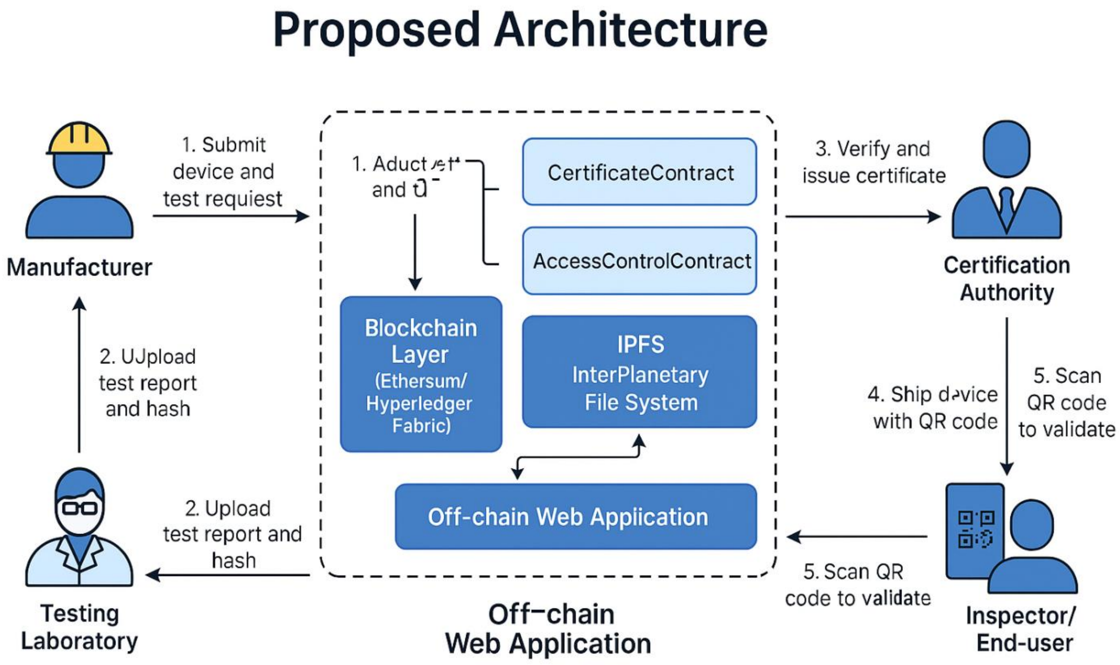
Proposed Architecture
Manufacturer
1. Submit device and test requiest
1. Aduct
and
CertificateContract
AccessControlContract
Blockchain Layer (Ethersum/ Hyperledger Fabric)
IPFS InterPlanetary File System
Off-chain Web Application
3. Verify and issue certificate
Certification Authority
2. UJpload test report and hash
Testing Laboratory
2. Upload test report and hash
4. Ship device with QR code
5. Scan QR code to validate
5. Scan QR code to validate
Inspector/ End-user
Off-chain Web Application

Figure 2: Proposed Architecture for Blockchain-based Certification Platform for Explosion-Proof Devices

3.1 Stakeholders

The digital certification platform Below is a summary of four major stakeholders in significant role of a trustful, transparent and integrity certification process:

Manufacturer: The manufacturer of the explosion-proof device (EXP-dev) starts the certification process by introducing EXP-dev's technical specs and design papers to the platform. The basic intention is to achieve an attested and tamper-proof certificate for the fulfilling of the explosion-protection requirement. A manufacturer interacts with this system by means of a user interface (UI) for submitting device data and requesting tests and evaluation.

Testing facility: One of our accredited third-party testing facilities carries out a thorough analysis of the device to determine whether it satisfies explosion-proof requirements ATEX or IECEx. These labs upload the test reports and data-sets derived from them to the decentralized storage system (IPFS). The respective hash of the test report is then stored on the blockchain for auditability and immutability, enhancing the credibility of the test results and strengthening trust among all parties involved.

Certification body: The "BaZ certification body" audits the documentation and test reports. When validation is successful, the authority will also generate a digital certificate on a blockchain via a smart contract. And it records cryptographic signatures to avoid counterfeiting it. The authority can also revoke or update certificates using the same smart contract logic, so that device certifications can be managed dynamically.

End-user/Inspector: On-site at deployment or inspection, end-users such as safety officers or regulatory inspectors utilize the system to confirm the certificate is authentic and accurate. That is usually achieved by scanning a QR code on the device, and, subsequently, certification data is fetched from a mobile or web application on the blockchain. This implementation allows for fast, transparent and independent verification.

3.2 Architectural Components

The Blockchain-Based Certification Platform We propose to implement the blockchain-based certification platform, which consists of several major architectural layers and components working together to build a tamper-evident, scalable, and decentralized system to certify the explosion-proof devices.

Blockchain Layer: The middle layer of the system is a blockchain module, built on top of blockchains such as Ethereum or Hyperledger Fabric. This layer records hashes of jawari's certification docs and manages the code logic of jawari certificate issuance and revocation by smart contract. The nonmodifiable ledger of blockchain guarantees that once information has been entered it cannot be changed or removed, so the record of certification history remains secure from tampering or fraud.

Smart Contracts: There are two main smart contracts that govern the operations of the blockchain:

- **Certificate Contract** is responsible for generation, addition and revocation of new device certificates. It references the on-chain document hashes, timestamps every action and provides an auditable trail of evidence.
- **Access Control Contract**: Controls user roles and permissions, so that only specific actors (e.g. certification authorities or test labs) can execute critical operations such as certificate issuance and test result upload.

Inter Planetary File System (IPFS): Since artifacts being certification documents, eg test report, design specifications, and evidence of compliance, could be of high size, they are stored off chain in a decentralized storage system like IPFS. On the blockchain, a record is made for Content Identifier or CID for every uploaded file by the hash. This enables the documents to be accessible and verified without burdening the blockchain with cumbersome data.

Off-chain Web Application An off-chain, user-friendly web application, that enables stakeholders to interact with the distributed ledger. The application is equipped with a dedicated interface meant for every role of the various stakeholders, whether it’s a manufacturer, lab technician, certification official or an inspector. It speaks to smart contracts through libraries like Web3. js or Ethers. js and provides a secure, real-time platform for running blockchain transactions by hiding the complexity.

3.3 Data Flow

Certification itself is realized as a set of steps performed by the involved players and system entities, coordinated by smart contracts and decentralized technologies. The overall flow of the data from one end to another is as follows:

Manufacturer Submission – A manufacturer logs Mad Ex Form Online into the Web application and registers a new explosion-proof device and places a request for certification testing. Device metadata and design files are shared on IPFS and the hash is made available to the testing lab.

Laboratory Testing and Reporting: The testing laboratory authorized carries out the necessary checks on equipment. Test reports and ratings are uploaded to IPFS when the test is finished. The hash of the report on IPFS is then posted to the blockchain in the form of a transaction and is verified using the Access Control Contract to verify the credentials of the lab.

Certificate Issue: after reception of the uploaded hash, the Certification Authority validates it, when positive, makes a request to the Certificate Contract to issue a digital certificate. This hash chain carries metadata about the device (the device ID, the issuing authority, the IPFS hash of the report, and the issuance time) and present information about the expiration of this certificate. The certificate is stored on the blockchain for tamper-proof access.

QR Code Creation and Device Marking: An individual QR code is generated including a hyperlink to, or identifier for, the blockchain transaction of the certificate. This code is hardwired into the certified apparatus. Any changes or cancellations to the certificate will be included in the blockchain state and can be checked with subsequent scans of the QR code.

On-Site Verification: Inspectors or field end users can simply scan the QR code with a mobile or web app. This app sends a blockchain query to the blockchain to obtain the current state of the certificate and checks its authenticity by comparing with the stored smart contract details and the IPFS hash. This achievement provides a rapid, certifiable means of verifying devices that does not depend on private or proprietary organization databases.

This structure provides a clear efficient and tamper resistant way to certify explosion proof devices. Through the use of blockchain, smart contracts, IPFS, and intuitive GUIs, this system solves some of the major issues in today's certification processes like document falsification, non-optimized auditing and delayed certification status updates.

4. Prototype Implementation and Results Interpretation

To prove feasibility and effectiveness of the proposed blockchain-based certification architecture, we implemented a prototype with a set of popular open-source tools and blockchain infrastructure. The objective was to recreate the entire certification journey — from equipment registration to certification issuance and field validation—without compromising user experience, transparency, or confidence, through decentralized solutions.

4.1 Technology Stack

The core components used to implement the prototype are related to the following:

- **Ethereum (Goerli Testnet):** Ethereum was chosen as the blockchain as it has a mature infrastructure, active developer community, and support for programmable smart contracts. Development on Goerli The Goerli testnet was used during development to avoid real transaction fees, while still keeping behaviour similar to the mainnet. Smart contract coded in Solidity and deployed, for the management of certificate issuance, revocation, and role-based access control.
- **IPFS (InterPlanetary File System):** IPFS served as the decentralized storage layer for heavy certification documents like test reports, design blue prints, compliance evaluations. Files that are uploaded to IPFS are content-addressed, and produce a CIDs – a unique cryptographic hash, which is saved

in the blockchain, to preserve the immutability and the verifiability of the data.

- **React. js and Web3. js frontend:** The front-end was developed on React. js to provide modularch, responzive, and interactive user interface specifics to the role Manufacturers, Testing Laboratories, Certification Authorities, and Inspectors. The Web3. js library was embedded to facilitate browser-based blockchain communication, in particular interacting with smart contract functions, and fetching on-chain certificate information.
- **Metamask Wallet**: User authorization and transaction signing was handled by Metamask browser wallet. Participants linked their Ethereum wallets with Metamask, which provided a way to safely sign blockchain transactions without needing to expose private keys to the application. Centralized credential management is not required with this decentralized identity model, thus increasing the security of the platform.

4.2 Performance Results

The prototype was tested in a controlled environment against the Goerli testnet with different simulated stakeholders to test for real world interactions. The results are given in table 1. The performance and utilization are summarized with the following metrics:

Table 1: Performance Metrics of the Blockchain-based Certification Platform Prototype

Metric	Description	Result
Certificate Issuance Time	Time taken from test report submission to certificate issuance, including IPFS upload and Ethereum transaction confirmation.	~4.8 seconds
Verification Time	Time taken by end-users/inspectors to scan QR code, retrieve certificate metadata from blockchain, and match IPFS hash for validation.	< 2 seconds
Cost per Transaction	Average gas fee incurred per certificate issuance transaction on the Goerli Ethereum testnet. Serves as an estimate for mainnet transaction cost.	~0.0004 ETH

Certificate Issuance Time

The average time consumed from when a test report was uploaded by the lab to when the issuance of a blockchain certificate by CA was successfully completed was about 4.8 seconds. This takes into account the time it takes to upload the report to IPFS, perform the smart contract transaction and confirm the block onto the Ethereum testnet. That amount of delay is quite acceptable for an industrial environment, and not a huge amount for tamper-proof verification.

Verification Time

The verification process—usually performed in the field by inspectors or end-users—put speed first. When scanning a device QR code, the app fetches the certificate metadata from the blockchain and verifies the IPFS hash matches the report being pointed to. Response time for the process was also relatively quick, with an average response time of less than 2 seconds this afforded a real-time verification with negligible overhead.

Cost per Transaction

A small gas fee, estimated to be around 0.0004 ETH per transaction (for minting a certificate, for example), was charged for every operation on the Goerli testnet's blockchain. Testnet transactions have no actual monetary value, however, and this figure should give you fairly accurate idea of the gas cost on the Ethereum main net under current market conditions. Further cost optimization could consider l2 solutions like Polygon or zkRollups or migrating to permissioned networks like HL Fabric for cost sensitive deployments.

Comparative analysis of traditional vs. blockchainbased certification systems is presented in table 2 and figure3. The migration to the blockchain solution would provide many advantages over the conventional certification method, including increased efficiency, security, and global usability. The issuance time, generally between 2 ~ 4 weeks in the existing systems by manual review, document submission, and liaison among agencies, is significantly decreased to less than one day using the blockchain system. This acceleration is achieved through automation, via smart contracts as well as instant data verification.

Table 2: Comparative Analysis of Traditional vs. Blockchain-based Certification Systems

Metric	**Traditional**	**Proposed Blockchain System**
Issuance Time	2–4 weeks	< 1 day
Tamper-proof Records	No	Yes
Traceability	Limited	Full
Cross-border Recognition	Manual	Instant & digital

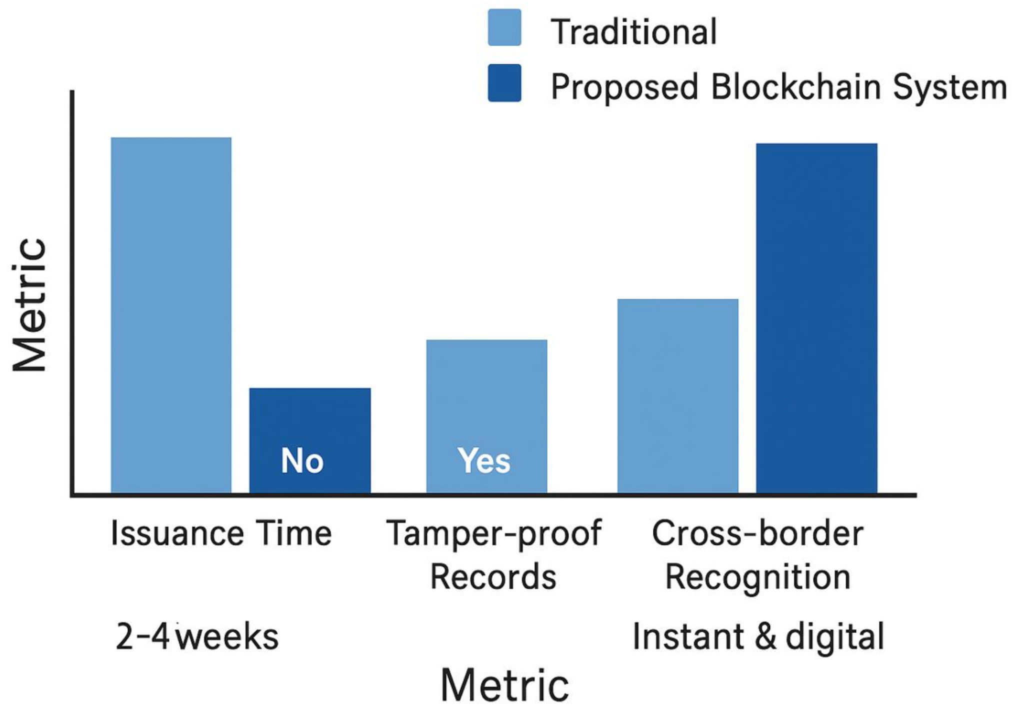

Figure 3: Comparison of Traditional vs. Blockchain-based Certification Systems

With respect to tamper-proof record keeping, current systems use centralized databases and have paper based certificates which can be forged, lost or tampered with. In comparison, the blockchain platform provides indestructible and proofed data that are cryptosecured, being tamperproof and providing trust between all stakeholders.

The second major step forward was in traceability. Conventional certification mechanisms offer only partial traceability, which may be obtained through manual follow up or written statement from certificating authorities. The proposed system adds full traceability to the mix, where each transaction is stored transparently in the blockchain and can be easily audited whether that was testing, approval, or revocation.

Finally, traditional models for recognizing qualifications across borders requires manual verification and operation of multiple regulatory regulator overlays—leading to delays and inconsistencies. Blockchain allows certification information to be immediately and digitally verified on any border,- streamlining international compliance and encouraging global compatibility.

The successful deployment of the prototype demonstrated the following advantages:

- **Security:** Immutable storage of certification data and cryptographically signed smart contracts reduced the risk of certificate forgery or manipulation.
- **Transparency:** Stakeholders could independently verify actions on the public blockchain, ensuring accountability.
- **Decentralization:** By eliminating reliance on centralized databases or manual verification chains, the system improved operational resilience.
- **Scalability:** The modular design allows integration with other standards bodies, additional devices, and various inspection workflows.
- **User Experience:** The React-based frontend and Metamask integration enabled seamless interaction without requiring users to have in-depth blockchain knowledge.

5. Conclusion

The paper introduced an architecture and implementation of a blockchain-based certification platform specialized in explosion-proof device, aiming to solve the problems in traditional certification: inefficiency and security in this field. The system automatically issues and revokes certificates using Ethereum smart contracts, uses IPFS decentralized storage as an efficient and fast method for storing large format tests, and uses a role-based web interface that allows manufacturers, testing laboratories, certificate authorities, and field inspectors to easily interact with the system. Selective results from the prototype implementation demonstrate remarkable enhancements in performance and security. the average of certificate issuance of 4.8 seconds, the average verification time below 2 seconds, the average transaction cost was about 0.0004ETH per transaction. These results represent a radical reduction in the 2-4 weeks required under current processes, and achieve near real-time (.1 second for a certificate) certification and verification, immutable record keeping and universal interoperability facilitated through blockchain infrastructure. Furthermore, the system proved to have a powerful tamper-proof certification, end-to-end traceability and instant cross-border validation healthcare or combustion-proof industries. The modular design supports the possibility of future compliance protocols and international regulators.

In future work, the system can also be further developed by incorporating layer-2 blockchain platforms (eg., Polygon, zkRollups) to lower the transaction fees, or by deploying the system on permissioned platforms (e.g., Hyperledger Fabric) for enterprise scenarios. Advanced features include AI-backed document verification, zero-knowledge proofs for privacy-oriented verification and industrial IoT connectivity for compliance monitoring in real-time.

References

[1] Z. Liang, K. Zhou, R. Gao, and K. Gao, "Special Equipment Safety Supervision System Architecture Based on Blockchain Technology," Appl. Sci., vol. 10, no. 20, p. 7344, 2020.

[2] F. Ghovanlooy Ghajar, A. Sikora, and D. Welte, "Schloss: Blockchain-Based System Architecture for Secure Industrial IoT," Electronics, vol. 11, no. 10, p. 1629, 2022.

[3] Q. Yang et al., "Secure Blockchain Platform for Industrial IoT with Trusted Computing Hardware," arXiv preprint arXiv:2110.15161, 2021.

[4] G. Rathee, F. Ahmad, N. Jaglan, and C. Konstantinou, "A Secure and Trusted Mechanism for Industrial IoT Network using Blockchain," arXiv preprint arXiv:2206.03419, 2022.

[5] R. Xu et al., "BlendMAS: A BLockchain-ENabled Decentralized Microservices Architecture for Smart Public Safety," arXiv preprint arXiv:1902.10567, 2019.

[6] S. Suhail et al., "Blockchain-based Digital Twins: Research Trends, Issues, and Future Challenges," arXiv preprint arXiv:2103.11585, 2021.

[7] Y. Zhou, "Industrial Internet Sensor Node Construction and System Construction Based on Blockchain Technology," J. Sensors, vol. 2023, Article ID 6137395, 2023.

[8] Y. Zhang et al., "Research on the Construction of a Blockchain-Based Industrial Product Full Life Cycle Information Traceability System," Appl. Sci., vol. 14, no. 11, p. 4569, 2022.

[9] D. Li et al., "High-performance blockchain system for fast certification of manufacturing data," SN Appl. Sci., vol. 4, no. 25, 2022.

[10] M. Shen et al., "Blockchain-assisted secure device authentication for cross-domain industrial IoT," IEEE J. Sel. Areas Commun., vol. 38, no. 5, pp. 942–954, 2020.

[11] D. Li et al., "Blockchain-based authentication for IIoT devices with PUF," J. Syst. Archit., vol. 130, p. 102638, 2022.

[12] P. C. Sharma et al., "Secure authentication and privacy-preserving blockchain for industrial internet of things," Comput. Electr. Eng., vol. 108, p. 108703, 2023.

[13] R. Saha et al., "DHACS: smart contract-based decentralized hybrid access control for industrial internet-of-things," IEEE Trans. Ind. Inform., vol. 18, no. 5, pp. 3452–3461, 2022.

[14] J. Cui et al., "An anonymous and outsourcing-supported multiauthority access control scheme with revocation for edge-enabled IIoT system," IEEE Syst. J., vol. 16, no. 4, pp. 6569–6580, 2022.

Citation: Sukruthi Reddy Sangannagari. (2025). Architecture for a Blockchain-based Certification Platform for Explosion-Proof Devices. International Journal of Computer Engineering and Technology (IJCET), 16(2), 498-515.

Abstract Link: https://iaeme.com/Home/article_id/IJCET_16_02_033

Article Link:
https://iaeme.com/MasterAdmin/Journal_uploads/IJCET/VOLUME_16_ISSUE_2/IJCET_16_02_033.pdf

✉ **editor@iaeme.com**