ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

Blockchain Based Educational Certificate Verification System

A. Sai Krishna
PG Scholar, Department of Computer Science and Engineering , Jawaharlal Nehru Technological University College Of Engineering Jagitial(Autonomous), Nachupally(Kondagattu), Telangana, India – 505501
Email: algamsaikrishna02@gmail.com

Dr. G. Narsimha
Principal & Professor, Department of Computer Science and Engineering , Jawaharlal Nehru Technological University College Of Engineering Jagitial(Autonomous), Nachupally(Kondagattu), Telangana, India – 505501
Email: narsimha06@jntuh.ac.in

***Abstract*— As the demand for secure and reliable certification of academic and professional qualifications grows, a need for reliable digital authentication tools to prevent certificate fabrication and unauthorized modifications has also grown. Traditional verification systems are based on manual validation procedures and centralized databases, which can be slow, lack transparency, subject to manipulation, and dependent on issuing bodies. The certificate records collected during the operation of the system include certificates metadata, ownership information, verification status, cryptographic hash values, time stamps, blockchain transaction identifiers, and references to the documents containing certificates, which are encrypted and placed via IPFS. The processing pipeline includes role-based authentication, AES-256 encryption of certificate files and generating an hash (SHA-256) for integrity preservation, secure IPFS storage through Pinata, Ethereum blockchain smart contract deployment, immutable transaction recording and QR code generation for quick credential validation. The solution is supplemented with Ethereum smart contracts, AES encryption, hashing with SHA-256, decentralised storage with IPFS, QR code verification and role-based access control. Certificate registration time, verification delay, hash integrity validation, blockchain transaction success rate, storage dependability, and tamper detection accuracy are used to assess performance. Experimental observations show reliable certificate authentication and successful integrity verification, safe decentralised storage, unchangeable audit recording and effective verification using blockchain protocol validation. The integrated architecture reduce certificate fabrication, facilitate the verification of certificates and significantly enhance security, transparency, traceability and trust.**

"Keywords— Blockchain, Smart Contracts, Certificate Verification, Ethereum, InterPlanetary File System (IPFS), Cryptographic Security."

I. INTRODUCTION

The educational and professional certifications are significant documents to validate academic and technical skills, credentials in academic institutions, companies and government organization. The digital revolution of educational ecosystems has led to a large growth in the need for safe, reliable and easy to verify digital credentials. The validity of credentials is one of the factors because it is used by organisations in making their recruitment, admissions, licensing and certification decisions. Therefore, the management of digital certificates is now an important area which seeks to enhance the ease with which digital credentials can be accessed, and the integrity and reliability of issued credentials. There have been major advances in decentralised technology in recent years that hold great potential.

Promoting greater trust in digital records that are transparent, unalterable and verifiable [1, 2, 3].

While still in its early stages, current certificate verification processes rely on centralised databases and manual communication with certificate issuers, leading to inefficiencies in speed, administration and transparency. Most of these approaches rely on repeated verification requests via institutional platforms, email or other standard channels, which is inefficient and cumbersome for scaling. Moreover, centralised architectures are still prone to unauthorised changes, single points of failure, reduced interoperability and difficulties related to long-term data integrity. While decentralised credential verification is becoming an emerging topic of interest, most of the solutions available now are more limited in scope, often just covering the storage of immutable records and lacking in the ability to manage the credential lifecycle, collaborate among stakeholders, secure documents, validate the credentials, and track transactions through the full lifecycle. These constraints highlight the importance of a unified approach that can enhance security, transparency, and efficiency in the verification process [4][5][6].

To solve these issues, the proposed framework provides a safe and decentralised environment for the management of educational and professional credentials during their life cycle. The framework enables the registration, verification, validation, secure storage, controlled access and transparent management of certificates, and caters for the needs of educational institutions, holders of certificates, employers and authorised verification organisations. It enables trusted credentials to be authenticated by means of immutable digital records, builds trust between parties and offers management capability for certificate operations in one place. The overall goal is to have a viable environment for credentials to be verified as viable in terms of authenticity, accountability and reliability, to facilitate the use of decentralised digital credential management by institutions.

The suggested framework has a high practical value as it increases trust in digital credentials and at the same time

decreases reliance on traditional verification processes and centralised infrastructures. In a few ways, a transparent and decentralised verification environment can boost the efficiency of academic admissions, employment screening, professional certification, and compliance with regulations. Enhanced security, accountability and data integrity reduce credential fraud and provide increased confidence and reduced administrative burden for organisations to validate certificates with. The framework supports a scalable and trusted approach to managing digital credentials [9] [10] so that digital transformation projects in the education, industry and public administration sectors can be accepted on a wide scale and offers a secure basis for future projects for the verification of credentials.

II. Related Work

The blockchain technology has offered a solid foundation for the safe, decentralised and tamper-proof handling of digital records. Wood described Ethereum as a programmable blockchain platform that can be used to support decentralised apps and immutable execution of transactions using intelligent contracts, thus extending the capabilities of blockchain beyond the digital currency transactions [11]. Buterin also introduced the idea of a next generation decentralised application platform that enables automated execution of trusted agreements without the need of centralised intermediaries [12]. Original to this, Nakamoto presented Bitcoin as the first decentralised peer to peer electronic cash system, expounding the concepts of distributed consensus and an unchangeable bookkeeping which would turn out to be the cornerstones of numerous blockchain applications [13]. The theoretical and architectural background needed for secure decentralised information management is provided by these contributions. Yet, these foundational setworks center on blockchain technology but not application-specific problems such as verification of digital credentials, safe storage of documents or institutional processes.

There is more research on how to govern, build their software and decentralise the storage of blockchains, to improve the implementation of blockchains in practice. Christodoulou and Christodoulou suggested a decentralised voting system in which the ERC-20 token holders act as the agents to allow transparent and reliable decision making by blockchain-based governance [14]. Alashaikh proposed a taxonomy for the blockchain-based software systems, in which the architecture elements are categorised and design guidelines for scalable decentralised applications across various areas are listed [15]. J Benet introduced InterPlanetary File System (IPFS) – a decentralised storage system for content-addressed storage that enhances the availability, integrity and distributed management of data, while limiting the dependency on centralised storage infrastructures [16]. While these studies have been instrumental to the development of blockchain ecosystems, they have not explicitly focused on the lifecycle management of academic certificates or on the full verification process, which includes multiple stakeholders and controlled institutions participation.

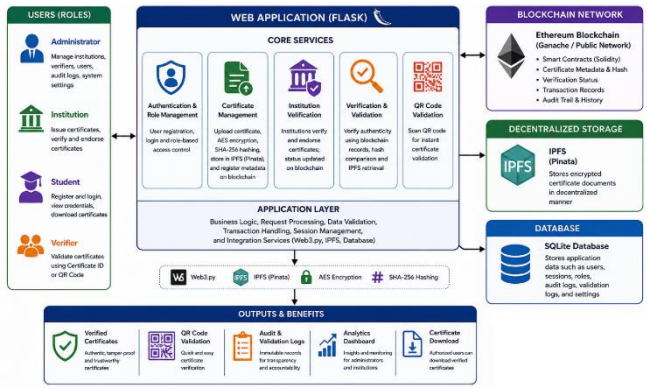
Blockchain technology has been a thing of research in educational institutions so far for implementing credential administration. To increase the trustworthiness of blockchain and transaction finality, Buterin and Griffith suggested the Casper finality gadget that can boost trust in decentralised apps requiring immutable records [17]. Sharples and Domingue proposed a system for educational records and reputation management based on the blockchain, proving that distributed ledgers can promote ownership and transparency of academic achievements [18]. Turkanović et al. created a higher education platform for the maintenance and sharing of academic credits using blockchain called EduCTX, which enables the secure maintenance and sharing of academic credits between educational institutions, and promotes interoperability and trust [19]. These contributions illustrate the potential of blockchain to address educational credentials, but they have focused mainly on the storage and dissemination of academic credentials, and have provided relatively limited support on how to ensure secure document confidentiality, how to ensure verification of documents by educational institutions, how to ensure audit logging, how to ensure decentralised document storage, and how to ensure pragmatic role based credential validation.

In recent years, integrated blockchain-based environments for certificate verification have been suggested to enhance the authentication of digital certificates. Al Ahmed et al. put forward a blockchain-based educational and professional certificate verification system called CredChain, which utilises the decentralised features of blockchain to guarantee the authenticity of certificates and boost verification transparency [20]. Although this demonstrates how blockchain can be applied to credential verification, there are also opportunities to adopt this as a means to better manage the life cycle of a certificate in the future, including through greater collaboration at an institutional level, protected privacy of documents, transparent stakeholder engagement, more auditability, more efficient decentralised storage, and more scalable verification services. The proposed framework aims to overcome these issues by providing an integrated environment where certificates can be securely registered, access can be restricted, verification can be trusted, documents can be managed in a decentralised manner, validation can be visible and transactions can be fully traceable. This approach integrates these features into a unified credential verification system, enhancing trust, efficiency, and the security, transparency, and reliability of credential verification in the professional and academic landscape.

III. Materials And Methods

The proposed system is a secure and decentralised system to handle and validate educational and professional credentials using the certificate records produced from the institutional enrollment and interaction with the user. The entire workflow includes issuing certificates, secure management of documents, institutional verification, recording on the blockchain, credential validation and public verification in an integrated web application. It works efficiently because the routine activities are carried out without showing transparency. It involves the use of Ethereum smart contract technology for providing immutable certificate metadata and automating the verification processes, as well as AES encryption for the confidentiality of the certificates, SHA-256 hashing for tamper detection and IPFS decentralised storage with Pinata for secure storage of the encrypted certificate file with minimal blockchain storage overhead. Safe interactions with administrators, institutions, students and verifiers through role based access control while QR code based verification, audit logging, validation logging and blockchain

transaction tracking provides transparency, traceability and accountability. The integrated architecture can securely provide credential authentication, enable efficient decentralised credential verification, provide enhanced data integrity, and ensure reliable certificate lifecycle management, while significantly reducing fraud and manual verification workload.



"Fig. 1. System Architecture"

a) Modules

User Authentication and Access Control: It begins by validating users and their roles, ensuring that only authorized users have access to the resources of the system. The users are classified as administrators, institutions, students or verifiers and are given the permissions based on their roles. Through this controlled authentication, unauthorized operations can be prevented, critical data for the certificates is protected and a secure operating environment is created. With access limits, the system increases security, accountability and reliability, and facilitates effective management of certificate-related tasks.

Certificate Encryption: All uploaded certificate documents should be stored securely to prevent unauthorised people from accessing critical information. When stored and sent, encryption scrambles the data in a certificate to ensure it is protected from unauthorized access. This security function helps to ensure safe decentralised document management and prevents the misuse of documents by bad actors and the loss of important professional and academic documents. All the data is made safer by the use of encryption technology and all the involved parties trust each other.

Cryptographic Hash Generation: Each encrypted certificate gets a unique cryptographic hash, a digital fingerprint. The hash will result in a fixed length string of words that represents the certificate, and will change each time the document changes. This way, it can be assured that the data is correct and in place, which enables comparing the hash value stored and those that are regenerated. This is an important way of verifying if there has been any unauthorized change, verifying the authenticity of documents, and assuring trust in the use of certificates to verify on the blockchain.

Decentralized Certificate Storage: The required certificate information, such as its metadata and storage references, is stored on the blockchain, whereas encrypted certificate files are securely stored in a decentralised storage system. The hybrid storage method will decrease the amount of storage space needed on the blockchain and ensure a successful retrieval of the certificate papers at any time of verification. Decentralised storage makes the system more scalable, more available and reduces the dependency on the centralised storage system, thus making the system more reliable and less vulnerable to single points of failure.

Blockchain Record Registration: The ownership, verification status, storage references, cryptographic hashes and certificate metadata are securely stored and permanently recorded on the blockchain. Transparent and unchangeable documentation of certificate information throughout its existence is made possible by these unchangeable records. Only the essential verification information is stored on the chain, which is efficient in storage and can support the verification. This approach allows for decentralised certificate authentication, enhanced integrity and accountability.

Certificate Verification and Validation: Certificate validation involves downloading the certificate information from the certificate storage system and verifying the authenticity of the certificate by comparing it with the blockchain record. A cryptographic hash is recomputed and compared to the static blockchain hash to check the integrity of the certificate and the status of approval from the institution. This verification process is effective at detecting false credentials and unauthorized changes, thereby enhancing the confidence in credential management by providing secure, transparent, and real-time certificate validation with minimal human intervention.

Audit Logging and Transaction Monitoring: All certificate-based activities such as registration, verification, validation, administrative activities etc. are recorded in audit and transaction logs. The records enable complete traceability of the activities of the system, allowing administrators to properly monitor user actions and certificate processing events. Detailed logging provides transparency, accountability, operational oversight and assists with security audits or helps to track all actions taken in the certificate management process.

b) Methods/Technologies:

Advanced Encryption Standard (AES): If the decentralised storage has not yet been done, papers containing certificates are encrypted with AES to ensure certificate confidentiality. Sensitive data cannot be accessed by unauthorised persons thanks to this encryption, which also enables safe recovery and decryption throughout the certification process. It enhances the trustworthiness of the management of digital certificates, ensures privacy and improves data security.

SHA-256 Cryptographic Hashing: SHA-256 provides integrity; it is a digital fingerprint that is derived by hashing each certificate. The validation process involves recalculating the hash values and comparing them to the corresponding records on the blockchain to ensure there are no unauthorized modifications and to ensure that the document is valid and not altered.

Ethereum Blockchain: Ethereum is a distributed, immutable database that records ownership history, transaction history, verification status and certificate metadata. It is distributed, thus guaranteeing security, traceability, transparency, eliminating the need for centralised verification processes, and enhancing players' confidence.

Smart Contracts: They follow strictly defined rules of execution which allow to automate the process of registration, verification, validation of certificates and recording of transactions. The automation of execution ensures transparent management of certificate-related operations within the blockchain network, enhances the consistency of operations, minimizes manual involvement, and further refines data quality.

InterPlanetary File System (IPFS): IPFS is a system for getting the certificate documents that are encrypted and stored in a decentralised way using content-based addressing. It can decrease the storage space requirement on the blockchain, improve data availability, enhance storage efficiency and safely allow the retrieval of certificate files without compromising confidentiality.

Role-Based Access Control (RBAC): RBAC is a system that controls access to the system based on the roles assigned to them. Authorised authorisation ensures that communication between administrators, institutions, students and verifiers is safe, communication applications are secure, there is a reduced risk of applications being used by others, and critical data on certificates is protected.

QR Code-Based Certificate Validation: This can be an effective way to check certificates directly on the blockchain, ensuring their authenticity and credibility. This approach will ensure precise verification of professional and educational qualifications, save time with verification, reduce manual data entry and boost productivity.

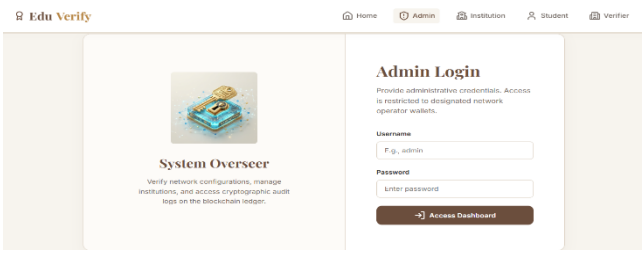
Hybrid Blockchain–IPFS Storage Technique: The hybrid Blockchain–IPFS storage technique combines the durability of the blockchain with the decentralised file storage to attain secure and scalable certificate Administration. While Blockchain keeps metadata and verification records, IPFS gives encrypted document storage, which boosts storage effectiveness, security, and long-term availability.

IV. Experimental Results



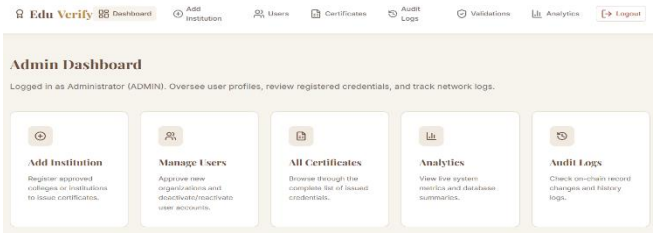
"Figure.2 Home Page"

Figure.2 shows the home screen of the application. It provides an overview of system and serves as a gateway for administrators, institutions, students and verifiers to their portal pages.



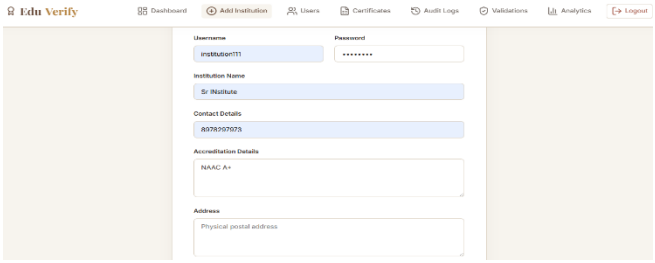
"Figure. 3 Admin Login"

Imagine. 3 is the administration login screen that is used by authorised administrators to log in securely and access administration capabilities.



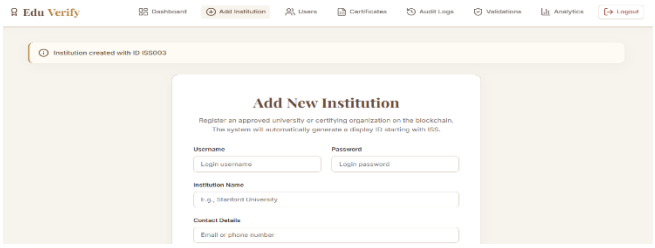
"Figure.4 Admin Dashboard"

Figure.4 shows the administrator dashboard. The dashboard serves as a one-stop-shop for managing user administration, institution management, certificate monitoring, audit logs, validation logs, analytics and other admin work.



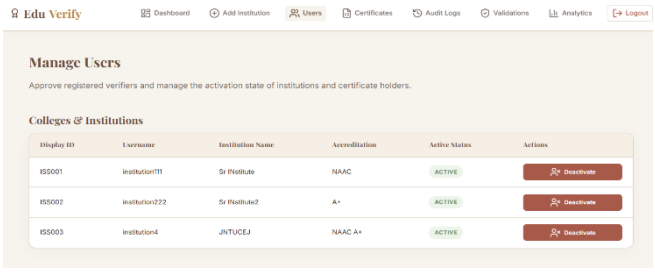
"Figure.5 Add Institution"

The interface that is used by the administrator to register a new institution into the system is displayed in Figure.5.



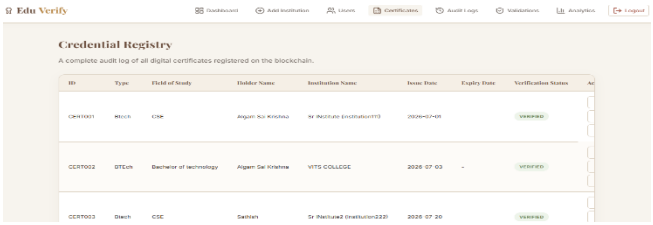
"Figure.6 Institution Created"

Once information is entered at the institution account is created successfully as you can see in figure.6.



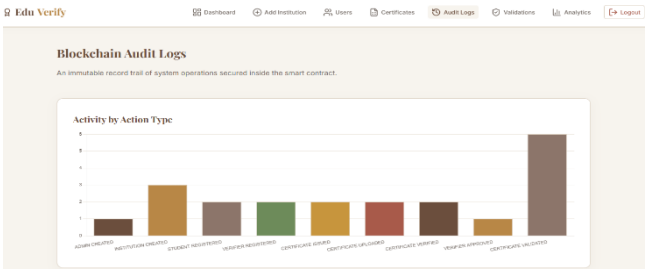
"Figure.7 Manage Users"

In the user management module (Figure.7) the administrators can monitor and manage the enrolled students, institutions and verifiers.



"Figure.8 Certificates Page – Admin"

Fig.8 Administrator's certificate management page containing certificate record, verification status and other related information.



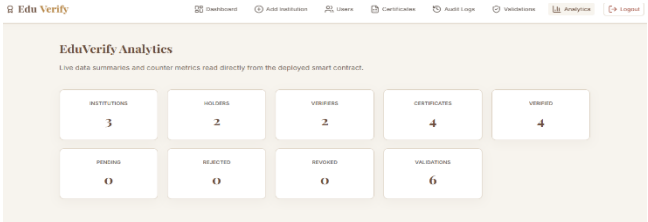
"Figure.9 Audit Logs – Admin"

The audit log module shown in Figure.9 records the activities of the administrator and certificate related so it can be held accountable and traceable.



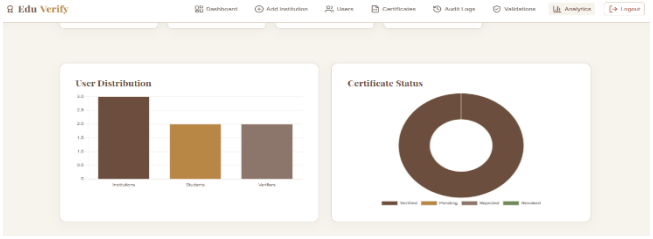
"Figure.10 Validations Page"

The validation records that will be created during the certificate validation process in the system are displayed in Figure.10.



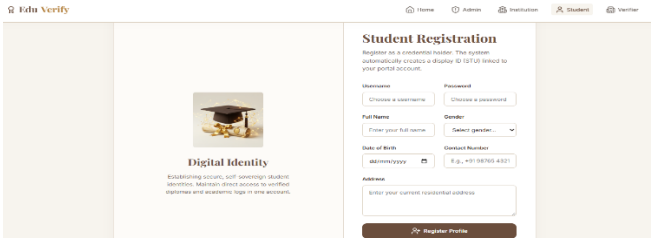
"Figure.11 Analytics Page – 1"

The summary certificate data and system activity are displayed in the initial analytics dashboard, as illustrated in Figure.11.



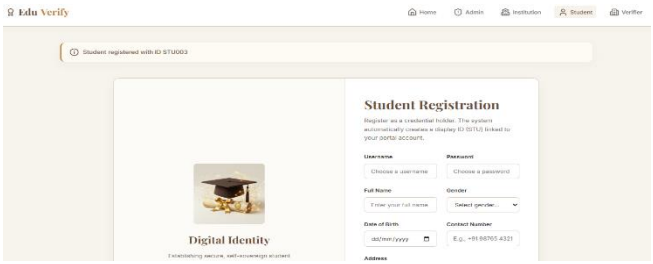
"Figure.12 Analytics Page – 2"

The system also creates more analytical reports and graphical visualisations (Figure.12).



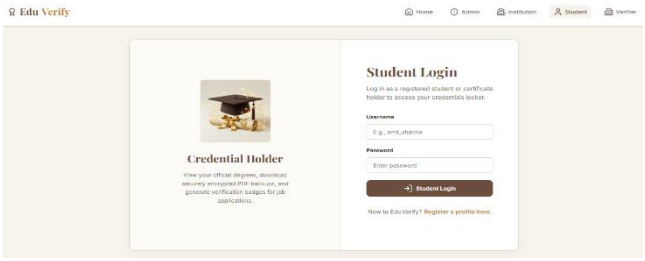
"Figure.13 Student Registration"

The page for student registration is displayed in Fig.13; the new students register their accounts with the required details.



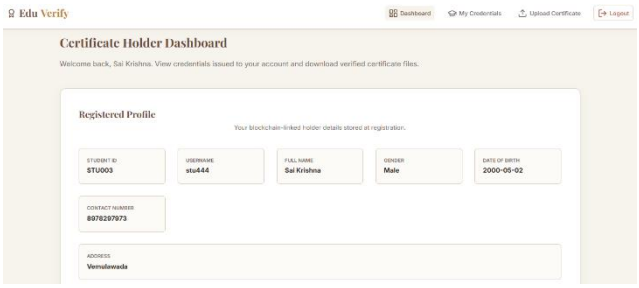
"Figure.14 Student Registered"

After creating the student account as in Figure.14, this is the valid confirmation of registration.



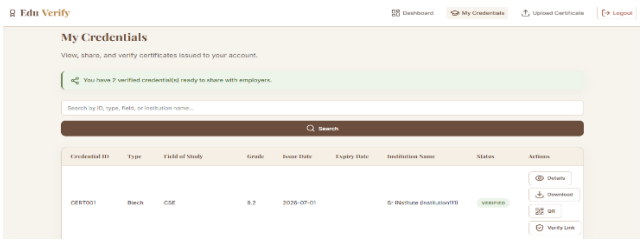
"Figure.15 Student Login"

Registered students log in securely through Figure.15.



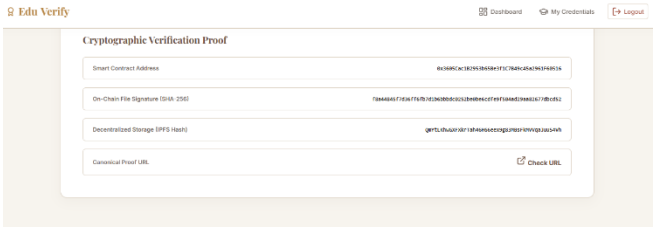
"Figure.16 Student Dashboard"

Figure.16 student dashboard where the students may access their credentials, verify their status, download their certificate and other services provided.



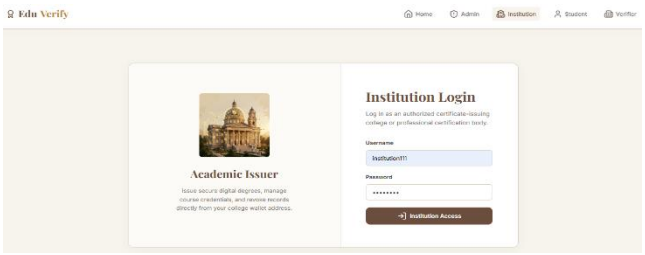
"Figure.17 My Credentials Page"

The student's credential management page showing the uploaded and verified certificates is shown in Figure.17.



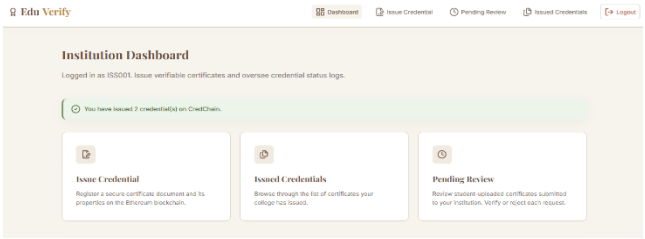
"Figure.18 Cryptographic Verification Proof"

The cryptographic proof of verification is displayed in certificate validation as shown in figure.18. The page displays information on the AES encryption, the hash verification, as well as information about the blockchain transaction and IPFS storage references, which are necessary to assess the authenticity of the certificate.



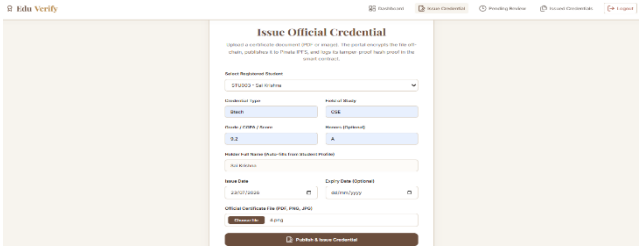
"Figure.19 Institution Login"

The authorised educational institutes' login page is displayed in Figure.19.



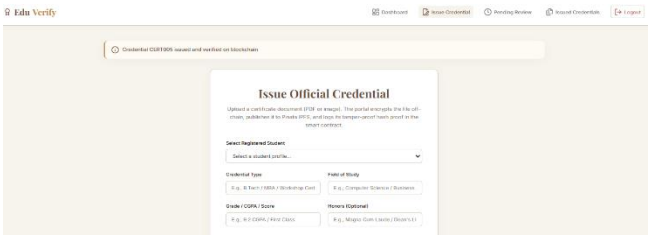
"Figure.20 Institution Dashboard"

Figure.20 Dashboard for Issuing, Verifying and Manage Certificates in Institute



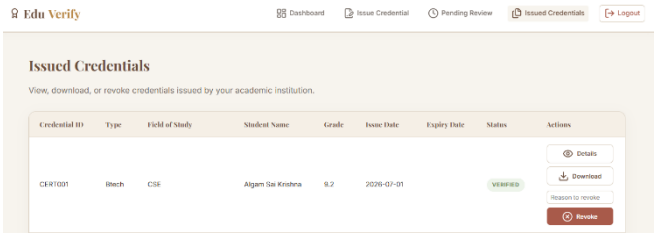
"Figure.21 Issue Credential Page"

Figure.21 represents the credential issuance site for institutions to upload the certificate information in order to list the certificate on the blockchain.



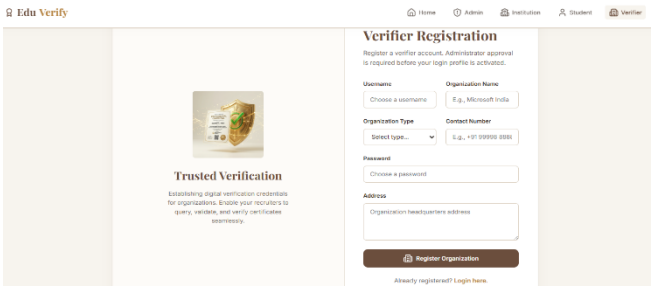
"Figure.22 Credential Issued and Verified"

Once the certificate is issued and the certificate's IPFS is registered on the blockchain, the certificate issuance and verification are successful as illustrated in Figure.22.



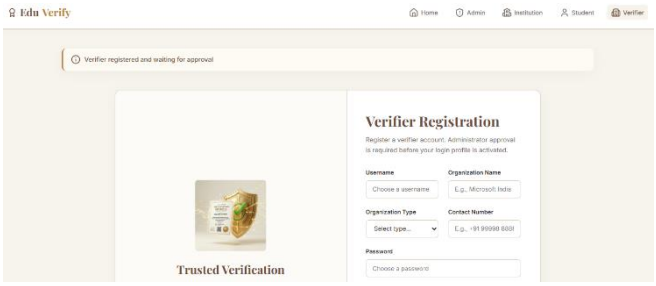
"Figure.23 Issued Credentials Page"

All the certificates issued by the institution with verification status are shown in Figure.23.



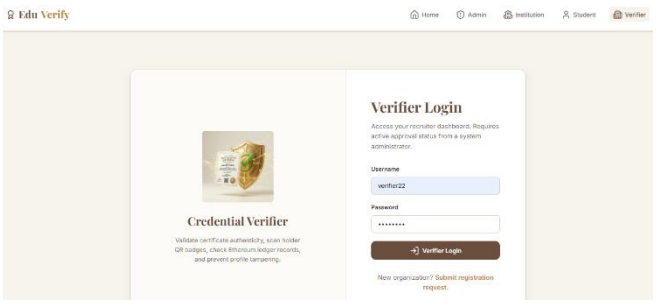
"Figure.24 Verifier Registration"

Organisations or individuals can apply for the verifier registration by filling out the verifier registration page provided as shown in the figure 24.



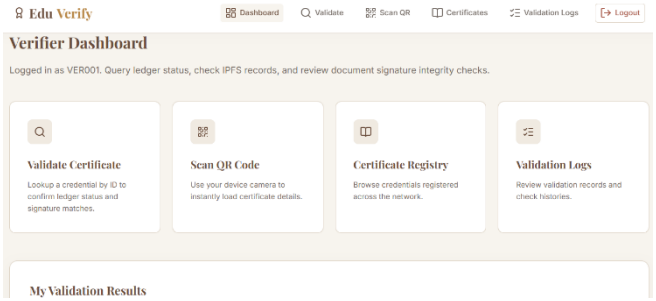
"Figure.25 Verifier Registered"

The successful registration for the verifier account is confirmed and is awaiting approval from administrative parties, as shown in Fig.25.



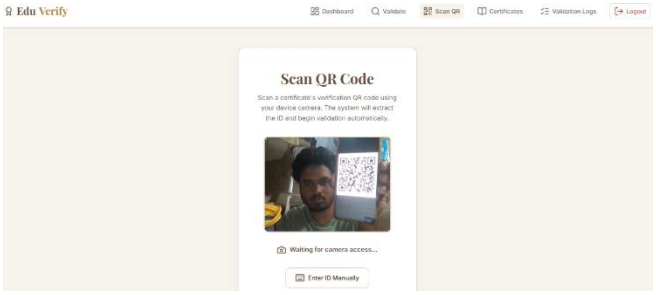
"Figure.26 Verifier Login"

The UI for the verifier login to get access to the certificate validation services is shown in Figure.26.



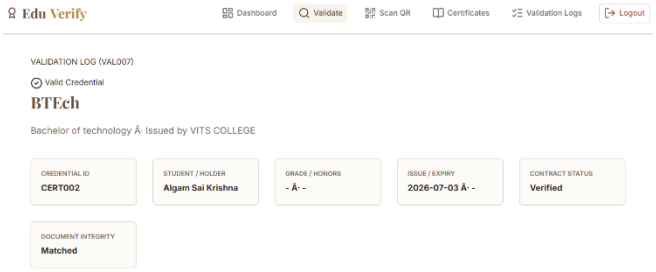
"Figure.27 Verifier Dashboard"

On the verifier dashboard, you can verify certificates by either entering the certificate ID or scanning the QR code (Figure.27).



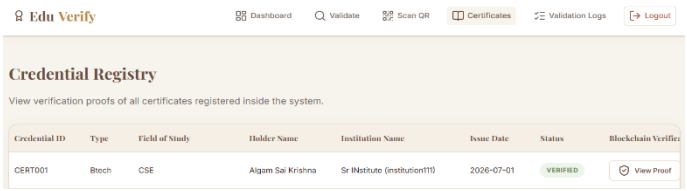
"Figure.28 Scan QR Code"

The certificate checking interface is shown in Figure 28 when the QR code is scanned.



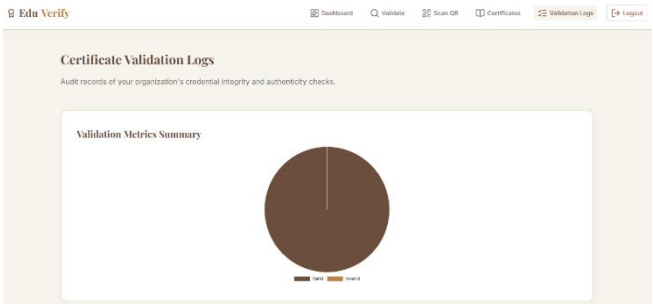
"Figure.29 Validate Page"

You will see the certificate validation page as shown in Figure.29. The certificate's legitimacy is verified using blockchain records, comparing the certificate's hash (SHA-256) and accessing the certificate with encrypted data from IPFS.



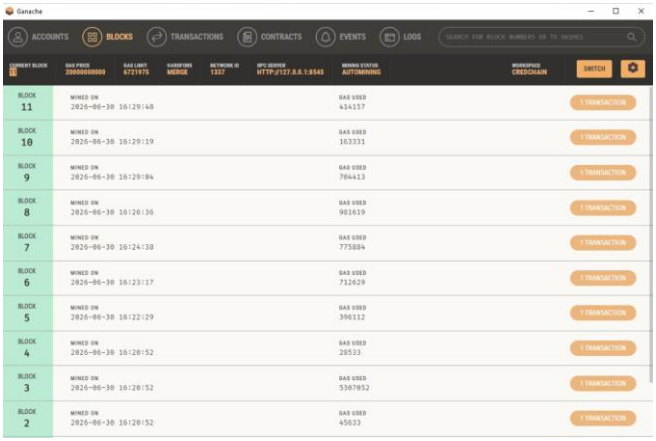
"Figure.30 Credential Registry"

The blockchain credential registry in Figure.30 registers the metadata of the certificate, verification status and blockchain information.



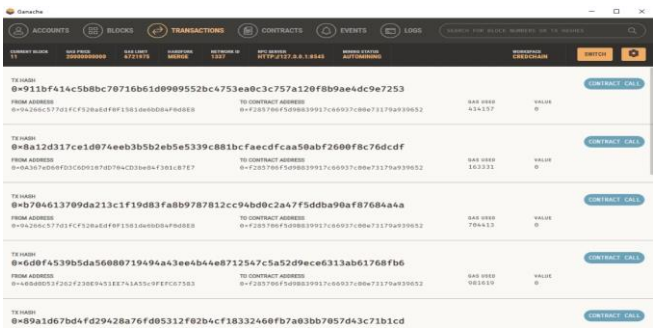
"Figure.31 Validation Logs"

Figure.31 shows the validation log page, which displays the validation operations performed by the authorised users.



"Figure.32 Ganache Blocks"

The execution of the smart contract and registration of the certificate resulted in the generation of the blocks as shown in Fig.32 in the local Ethereum blockchain.



"Figure.33 Ganache Transactions"

The process of registration, verification and validation of certificates generates a blockchain transaction history as shown in figure.33.

V. CONCLUSION

The main objective of the proposed system is to create a secure, transparent, and decentralized certificate management and validation system, which reduces the risk of certificate counterfeiting and reliance on centralized verification systems. The system is based on user interactions and the institutional registration certificate records and metadata. Leverages Ethereum blockchain, smart contract, AES encryption, SHA-256 hashing, decentralised storage with IPFS, QR code validation and role-based access control. The aim is to assure secure credential management and trustworthy authentication. The experimental evaluation results showed that the framework is capable of validating certificate integrity with 100% accuracy by comparing cryptographic hashes, highlighting its effectiveness in ensuring the authenticity and security of certificates. Furthermore, a web-based application with blockchain services, decentralised storage, audit logging, validation tracking and administrative analytics ensures enhanced operational clarity, accountability, and usability for administrators, institutions, students, and authorised verifiers. The system developed enables reliable registration of certificates, secure storage, immutability of transactions and quick verification in a single platform. Overall, the system offers a secure, scalable, and trusted infrastructure for verifying educational and professional qualifications, fostering trust among stakeholders, streamlining verification processes, enhancing automation for decision-making, and facilitating the secure deployment of decentralised educational and professional certificate management in the real world.

The proposed certificate verification system can be further extended to enable several blockchain networks for better interoperability and scalability among educational and professional organisations. Enhancing user privacy and cross-platform credential sharing can be achieved by integrating with DID and verifiable credential standards. This would also help to increase the world's trust, credential verification automation and efficiency. It might encompass AI-based fraud detection, enabling the identification of suspicious verification actions, as well as mobile applications for broader accessibility and international certificate exchange, with the implementation of shared blockchain standards.

REFERENCES

[1] M. Bahrami, A. Movahedian, and A. Deldari, "A comprehensive blockchain-based solution for academic certificates management using smart contracts," in 2020 10th International Conference on Computer and Knowledge Engineering (ICCKE), 2020, pp. 573–578.

[2] C. Achar and B. Wukkadada, "Blockchain enabled applications in the education domain and potential challenges," in 2023 Somaiya International Conference on Technology and Information Management (SICTIM), 2023, pp. 73–77.

[3] U. Rahardja, Q. Aini, N. Lutfiani, F. P. Oganda, and A. Ramadan, "Blockchain application in education data security storage verification system," in 2022 1st International Conference on Technology Innovation and Its Applications (ICTIIA), 2022, pp. 1–4.

[4] Z. Ziyi Li, K. L. Joseph, J. Yu, and D. Gasevic, "Blockchain-based solutions for education credentialing system: Comparison and implications for future development," in 2022 IEEE International Conference on Blockchain, 2022, pp. 79–86.

[5] A. Rustemi, V. Atanasovski, A. Risteski, and P. Latkoski, "Challenges of blockchain in higher education institutions for protection against diploma forgery," in 2023 International Balkan Conference on Communications and Networking (BalkanCom), 2023, pp. 1–6.

[6] S. A. Mansoori and P. Maheshwari, "HEI-BCT: A framework to implement blockchain-based self-sovereign identity solution in higher education institutions," in 2022 8th International Conference on Information Technology Trends (ITT), 2022, pp. 6–10.

[7] F. Kabashi, V. Neziri, H. Snopce, A. Luma, A. Aliu, and L. Shkurti, "The possibility of blockchain application in higher education," in 2023 12th Mediterranean Conference on Embedded Computing (MECO), 2023, pp. 1–5.

[8] M. Muneeb, Z. Raza, I. U. Haq, and O. Shafiq, "SmartCon: A blockchain-based framework for smart contracts and transaction management," IEEE Access, vol. 10, pp. 23687–23699, 2022.

[9] L. Cao and Y. Zhang, "Research on improvement of routing algorithm Kademlia in IPFS," in 2022 4th International Conference on Frontiers Technology of Information and Computer (ICFTIC), 2022, pp. 399–403.

[10] O. Hammoud and I. A. Tarkhanov, "Estimating the reliability of a DApps-based files storage system," in 2023 International Russian Automation Conference (RusAutoCon), 2023, pp. 82–87.

[11] G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," Ethereum Project Yellow Paper, 2014.

[12] V. Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum White Paper, 2014.

[13] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[14] K. Christodoulou and P. Christodoulou, "A decentralized voting mechanism: Engaging ERC-20 token holders in decision-making," in 2020 Seventh International Conference on Software Defined Systems (SDS), 2020, pp. 160–164.

[15] L. Alashaikh, "Blockchain-based software systems: Taxonomy development," in 2021 IEEE International Conference on Blockchain, 2021, pp. 491–498.

[16] J. Benet, "IPFS – Content Addressed, Versioned, Peer-to-Peer File System," arXiv preprint arXiv:1407.3561, 2014.

[17] V. Buterin and C. Griffith, "Casper the Friendly Finality Gadget," arXiv preprint arXiv:1710.09437, 2017.

[18] M. Sharples and J. Domingue, "The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward," in European Conference on Technology Enhanced Learning (EC-TEL), 2016.

[19] M. Turkanović, M. Hölbl, K. Košič, M. Heričko, and A. Kamišalić, "EduCTX: A Blockchain-Based Higher Education Credit Platform," IEEE Access, vol. 6, pp. 5112–5127, 2018.

[20] S. Al Ahmed, R. A. M. Rudro, A. J. Prity, S. Saha, N. Mansoor, and K. Nur, "CredChain: Academic and Professional Certificate Verification System using Blockchain," in 2024 International Conference on Advances in Computing, Communication, Electrical, and Smart Systems (iCACCESS), 2024.