2024 IEEE 4th International Conference on ICT in Business Industry & Government (ICTBIG) | 979-8-3315-1898-1/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICTBIG64922.2024.10911469

VaLiDiFy – Certificate Validation using Blockchain and AI

Bipin Kumar Rai
Dept. of CSE
Dayananda Sagar University
Bengaluru, India
bipinkrai@gmail.com
https://orcid.org/0000-0002-9834-8093

Bilal Ahmed NK
Dept. of CSE
Dayananda Sagar University
Bengaluru, India
notbilalahmed@gmail.com
https://orcid.org/0009-0007-1689-3025

Adarsh Priyadarshi
Dept. of CSE
Dayananda Sagar University
Bengaluru, India
adarshp0808@gmail.com
https://orcid.org/0009-0000-7082-8557

Abhinash Kumar Bej
Dept. of CSE
Dayananda Sagar University
Bengaluru, India
bejabhinash@gmail.com
https://orcid.org/0009-0005-1432-588X

Vivek S.H.
Dept. of CSE
Dayananda Sagar University
Bengaluru, India
viveksh4380@gmail.com
https://orcid.org/0009-0004-6247-097X

***Abstract*- The latest data demonstrates that 34% of resumes, 5% of academic certificates, and 23% of job applications in South Asian countries contain anomalies. The non-verification rate of academic certificates is found to be around 12.9% in certain developed countries. This emphasizes the issues pertaining to fraud with respect to certificate verification. The above figures demonstrate the need for a secure system that maintains the trust and transparency of credentials. To resolve this, we offer a robust solution that is based on Blockchain Technology for certificate validation by combining features of AI and advanced machine learning algorithms to enhance the verification process and thereby reduce credential fraud. The AI system detects anomalies or tampering attempts within each block; it also analyzes the pattern in block data, then verifies consistency and identifies suspicious changes, which may indicate manipulation of data. The user database is maintained through MongoDB. When compared to other approaches, the emphasis is on robustness through established cryptographic methods, which maintains its own secure database of hashes. Such an integration of technologies results in this cohesive system, ensuring efficient and secure digital certificate management as a scalable and adaptable solution. The focus on fundamental elements of blockchain makes it distinct when compared to more complex or isolated methods in other existing research works.**

Keywords- Blockchain, IPFS, AI, Smart Contract, PoA

I. INTRODUCTION

In both the professional and educational spheres, the problem of certificate counterfeiting has long existed. The Conventional approach for verifying the certificate is done manually. This discredits the honest efforts of the employees and poses a challenge for companies and universities in identifying the real and authentic certifications and qualifications. The need for a robust, tamper-proof solution to ensure the integrity of certificates is crucial to maintaining trust in educational and professional credentials. The traditional methods of managing and storing credentials are inefficient because there are chances of loss and damage that require significant administrative burden and operational costs. This makes a complex process both for certificate issuing and recipient parties. To solve the above problem, we propose a solution utilizing blockchain technology. It is a decentralized and distributed digital ledger technology that makes it an ideal solution for secure certificate management. Our system has been designed to store digital certificates on the blockchain, where each certificate is uniquely identified by their hash value. Any attempt to alter the certificate would be immediately detectable because it changes the hash value which no longer matches with the stored hash value inside blockchain. Smart contracts are used within the blockchain which further enhances the security and efficiency of the certificate issuance and verification process. It automates the process of certificate issuance, ensuring that certificates are only issued to individuals who meet specific criteria, thereby reducing the potential for any human error and fraud. Further, chaotic algorithms and SHA-256 have been employed for generating secure hash values from uploaded certificates which further enhances the security of digital certificates. The integration of InterPlanetary File System (IPFS) has been implemented for decentralized storage which enhances the security and accessibility of certificate data, ensuring that the certificates will be secured and retrieved when required. By leveraging these technologies, the proposed methodologies create a decentralized and transparent system for certificate validation, reducing the risk of forgery and improving efficiency of the verification process. The results obtained from these methodologies have been promising, demonstrating the potential of blockchain technology in revolutionizing certificate management systems. The proposed methodology creates a decentralized and transparent system for certificate validation. By leveraging these techniques there is reduction in risk of forgery and thereby improves efficiency of verification process the obtained results are promising as the demonstrate the potential of blockchain and AI in revolutionizing the certificate validation and management system. In Fig.1 describes the processing time of the certificates that indicates the effectiveness of blockchain-based solutions. However, the processing time of certificates in the traditional systems were

979-8-3315-1898-1/24/$31.00 ©2024 IEEE

Authorized licensed use limited to: Military Institute of Science and Technology. Downloaded on August 25,2025 at 02:48:40 UTC from IEEE Xplore. Restrictions apply.

high and inefficient. There was a drastic change in the graph after the implementing of blockchain technology. Which highlighted the efficiency and speed brought by the automated and decentralized verification process. This improvement has reduced the administrative overhead and also accelerated the issuance of certificates, ensuring timely verification for educational and professional credentials. From, the results had brought a clear idea of adopting blockchain technology in certificate management systems, which had provided a secure and streamlined approach to handling the certifications. Additionally, improvements such as data security, transparency, and efficiency were shown after the implementation of blockchain based system. Some prototypes were built on platforms like Ethereum, that have supported automated certificate credit adjustments and multi-step accreditation processes, which have proved the feasibility and effectiveness of these solutions. As the blockchain's nature is immutable which means, it cannot be altered or deleted, providing a permanent and tamper-proof record. Which provides trustworthiness of certificates. From the above advancements it highlight the potential of blockchain to enhance the reliability and legitimacy of certificates, ensuring a trustworthy system for the credential verification.

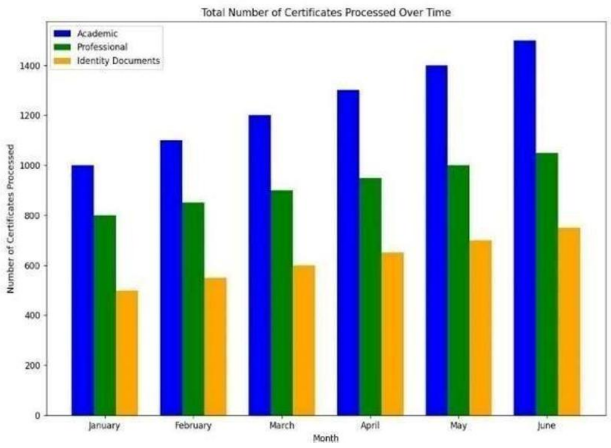

Fig. 1: Certificate Processing time.

A. Research Objective

The main objectives of the research work are as follows:

- Prevention of forgery and maintain the authenticity of the certificates which are achieved during the employment for validation.
- Designing a robust secured Blockchain system that can validate certificate through Smart contracts.

II. LITERATURE SURVEY

Blockchain technology first addresses the problem of certificate fraud by creating electronic file. This file contains the paper certificate and other relevant information. The database computes the hash value of this file, which is kept securely inside the block in the chain system. According to the authors of [1], the system will subsequently produce a QR code and an inquiry string code to be attached to the printed certificate. This allows the demand unit to verify the authenticity of the paper certificate via mobile phone scanning or website searches. Due to the blockchain's immutability, the technology greatly reduces the risk of certificate loss while also boosting the validity of various paper-based certifications. The issue of fake academic qualifications has long troubled the academic community. To address this, digital certificates are stored on the blockchain. Each university using this system will have a wallet address for transactions. The owner of the smart contract is the only one who can add universities. According to the authors of [2], after the institution uploads the data, it can create certificates with specific data fields using the system.

Each newly generated certificate is stored in the Interplanetary File System (IPFS), which provides a unique hash generated by the SHA-256 algorithm. The learner receives the generated transaction ID, and all related data including the hash and certificate details are documented on the blockchain. Using the IPFS hash stored with the data, anyone can view the original copy of the certificate and verify the certificate's credentials with the transaction ID. Decentralized applications and the potential advantages of blockchain technology hold significant value. The authors of [3] track the development of blockchain systems, beginning with a Bitcoin based decentralized ledger, which embodies the structure of the conventional blockchain. Bitcoin's main contribution is its capacity to eliminate duplicate spending, giving digital assets a unique and valuable position. The widespread use of Bitcoin enables the general public to use blockchain applications. Following Bitcoin is the decentralized smart contract platform, Ethereum. Ethereum aims to enhance the value of the blockchain network by enabling centralized smart contracts using Ether. Ethereum developers can use Solidity, a Turing-complete programming language, to create a variety of smart contracts, which are executable programs embedded inside blocks. Finally, the ideal blockchain application should be a decentralized application fully hosted on a peer-to-peer blockchain network. In other words, the ideal blockchain service or application should operate without requiring human intervention, leading to the creation of a Decentralized Autonomous Organization. A Decentralized Autonomous Organization is a business run by smart contracts programmed with rules and based on the blockchain. The system will be uploaded to the blockchain along with the degree certificate, the individual's complete profile, and all their behavioral patterns. The authors of [4] suggested that the student first seeks an e-certificate by uploading a certificate or their photo ID to the electronic certificate system. The user then receives a QR code generated by the system. When applying to a corporation, the user will only need to submit the QR code and certificate serial number obtained from the e certificate company. With the help of chaotic algorithm hash values are been created for the digital certificates. Which has a resistant characteristic, which provide a guarantee of authenticity and integrity of digital certificates stored on the blockchain. The algorithm used by the authors of [5], provides a good leverage and sensitivity to the initial conditions and also making the setting extremely resistant to manipulation, unlike conventional hashing algorithms like SHA-1. The risk of certificate fraud is reduced through the

Authorized licensed use limited to: Military Institute of Science and Technology. Downloaded on August 25,2025 at 02:48:40 UTC from IEEE Xplore. Restrictions apply.

creation of a transparent, decentralized, and a secured certificate validation system after the combination of this algorithm with blockchain technology. Such methods ensures the reliability and quality of digital credentials while offering a scalable solution.. By implementing SHA-256 algorithm with blockchain technology it gives us a safe and secure way to validate the certificates. Implementing smart contract has been advised which helps in automation of university registration and issuing certificates, underscoring the use case of blockchain technology for safe credential administration. The authors of[6] suggest, utilizing Inter Planetary File System (IPFS) to store certificate data and use SHA-256 hashing algorithm to ensure unique and unchangeable identities. In addition to this it focuses on issuing transaction IDs for quick and reliable certificate verification. The authors of [7] suggest Seamless integration of Hyperledger Fabric for optimal efficiency and management of educational certificates, creates a secure and non-changeable blockchain network. They suggest using IPFS for decentralized file storage, which helps in data security and ensuring user-friendly access in the certificate verification process. This integration puts a light on use cases of blockchain technology like security, efficiency, and reliability of systems used to verify educational certificates. The authors of [8] suggest that by integrating Elliptic Curve Digital Signature (ECDS) with blockchain which helps in automating procedures, cutting administrative costs thereby increasing effectiveness in certificate administration. They recommend using SHA-256 Algorithm, which is employed to verify digital signatures produced by ECDS and maintain data integrity. This standardized encrypted hash protects the data while producing same hash output for the same input. It is impervious to cryptographic assaults, such as collision and preimage attacks, as noted by the authors of [9]. We can note that several strategies for safeguarding user data and certificates are provided, as noted by the authors of [10]. These include the Secure E-Qualification Certificate System, which reduces the risk of hacking and saves storage, particularly when used nationally and e-certificates must be valid for life. Another strategy is the Cloud-based Graduation Certificate Verification Mode, whose main features are security, validity, and confidentiality, as the system will generate a corresponding QR code and inquiry string code to attach to the paper certificate. Lastly, Blockchain & Smart Contract for Digital Certificate will enable the demand unit to use website queries or mobile phone scanning to confirm the legitimacy of the paper certificate. The Blockchain-based Certificate System with Credit Self-Adjustment system allows employers to provide feedback based on the performance of their employees who hold various certifications. The authors of [11] suggest that BC-CS uses a proposed credit self-adjustment mechanism to automatically modify the certificate credits in response to the comments. A decentralized application prototype has been developed on an Ethereum network to verify the system's feasibility. The test results illustrate that the proposed solution can handle multi-step certification with automated certificate credit adjustment simultaneously. The literature emphasizes on blockchain's decentralized storage and immutable nature as a powerful tool for secure, scalable, and transparent certificate validation for reducing fraud. The implementation of Advanced cryptographic algorithm and methods like ECDS and SHA-256 further enhances reliability and trust on digital credential verification systems, highlighting its important role in professional and educational sectors.

III. METHODOLOGY AND PROPOSED WORK

A. Methodology

Validify proposes a methodology that uses a multi-layered system for certificate validation and security, integrating federated learning, decentralized storage, and blockchain technology to maintain integrity and prevent forgery. The initial step involves using a federated learning-based model to analyze certificate data for various inconsistencies. This decentralized approach allows the model to analyze data without centralizing sensitive information, enhancing privacy by mitigating data exposure risks. The model is trained on various nodes within the blockchain on features such as issuing institution, issuance date, course details, and digital signatures. It trains on a synthetic dataset created through various augmentation techniques and achieves an accuracy of 94% in detecting fraudulent patterns, effectively benchmarking against historical data. This initial validation step helps filter out 30% of all discrepancies before storing data on the blockchain, which increases the reliability of the stored data. Following the initial validation, data is stored on the InterPlanetary File System (IPFS), which generates a unique content identifier (CID) for each certificate. This CID ensures decentralized, tamper-free storage, allowing for retrieval based on content rather than location. The blockchain then organizes these validated records using Merkle Trees, providing a cryptographic structure for efficient data verification within the network. Any data alteration attempt is instantly detected due to the Merkle Tree's hash-based structure. To enhance Validify's permissioned environment, a proof-of-authority (PoA) consensus mechanism is employed, where designated authorities validate blocks, significantly reducing processing times and energy costs compared to Proof of Work. This choice enables the system to achieve block finality in under 5 seconds—an improvement over PoW's 20-30 seconds—and reduces computational demands by approximately 40%. Smart contracts, written to automate certificate issuance and management, govern all certificate transactions. These contracts enforce predefined issuance criteria, including course completion verification and institution accreditation, with an error rate below 1% in automated validation tests. Additionally, the smart contracts support real-time revocation, allowing institutions to update or revoke certificates efficiently. Validify's architecture—combining federated model-based validation, IPFS decentralized storage, PoA consensus, and smart contract automation—demonstrates a 60% improvement in processing efficiency and a significant reduction in administrative costs. This comprehensive approach ensures that certificates are issued and stored securely and remain tamper-free throughout their lifecycle, providing a scalable solution for trusted digital certification.

B. Procedure of Functioning

The functioning of Validify consists of several steps, as shown in Fig. 2, to ensure the secure issuance and verification of certificates. First, when a user or organization registers,

Authorized licensed use limited to: Military Institute of Science and Technology. Downloaded on August 25,2025 at 02:48:40 UTC from IEEE Xplore. Restrictions apply.

information is stored in the database, facilitating authentication. This registration process ensures that only verified individuals or organizations can access the platform. After the process is completed, the organization issues a certificate through the marking system, efficiently paving the way for smart contract implementation.

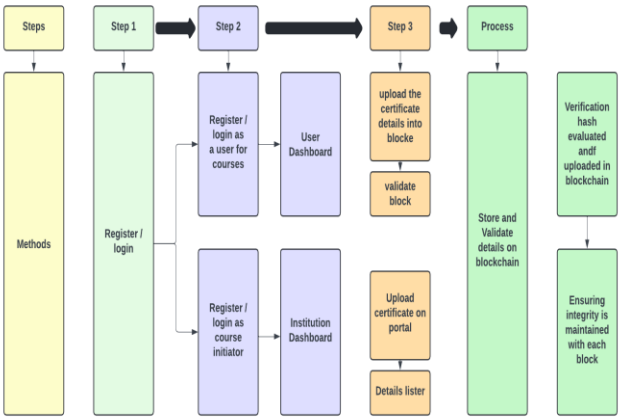

Fig. 2: Process flow.

Before issuance, certificate data is validated using a federated learning algorithm to protect data privacy while improving verification accuracy. Federated learning, using a decentralized approach, allows for the detection of anomalies in certificate data across multiple nodes without centralizing information. This process uses federated learning to compare new data with historical data to detect incorrect data templates. After verification, certificate information is stored on the blockchain. Each certificate is assigned a unique content identifier (CID) for storage on the InterPlanetary File System (IPFS), enabling tamper-proof, decentralized data retrieval. To verify the integrity of stored data, Validify replaces the proof-of-work mechanism with a more efficient proof-of-authority (PoA) mechanism, where blocks are authenticated using designated credentials. This shift to PoA ensures faster block finalization, reduces processing time, and conserves energy.

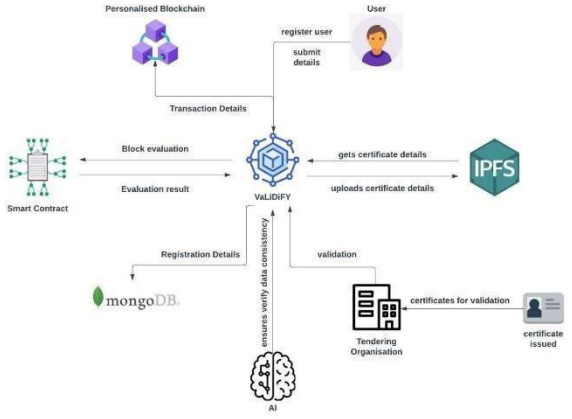

Fig 3: Sequence diagram.

C. *Marking System based Smart Contract*

To ensure a secure and efficient certificate issuance process, Validify replaces traditional transaction-based gas fees with a threshold-based qualification mechanism managed through smart contracts. This approach enforces predefined eligibility criteria directly within the blockchain framework, thereby eliminating the need for an arbitrary scoring system. Unlike the initial individually based marking system, this smart contract-based approach leverages credential verification as part of the certification process itself. Each certificate request is verified against the stored records, ensuring that the user has met all prerequisites without requiring additional "marks" or points. By incorporating this streamlined proficiency check, Validify increases both transparency and security, reduces complexity, and maintains consistency while protecting against manipulation. This approach aligns closely with blockchain principles, embedding all validation criteria within a distributed ledger that ensures all authentication transactions are consistently verifiable.

D. *Using Federated Learning to detect anomalies at issuance stage:*

Validify implements federated learning at the issuance stage of certificates to detect anomalies. This approach trains a decentralized model on historical certificate data from various participating nodes, allowing each institution to contribute to the model without exposing sensitive data. The model learns patterns from valid certificates by training on key features such as course name, issuing institution, certificate hash, and user details, while training on a synthetic dataset based on real-time scenarios, achieving a detection accuracy rate of approximately 94% in identifying potentially fraudulent certificates. During issuance, each new certificate is assessed by the federated model, assigning an anomaly score to detect deviations from known patterns. Certificates with an anomaly score above a predefined threshold (around 3% of cases) are flagged for further investigation. Fig. 4 illustrates this process, with normally distributed data points representing valid certificates, while the anomaly map highlights areas of potential discrepancies. This approach ensures rapid detection of fraudulent or erroneous certificates, bolstering the system's integrity and reducing error rates by 87%.

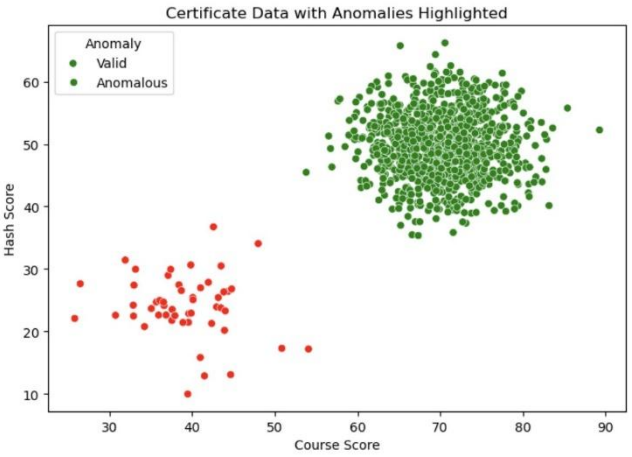

Fig 4: AI Integration

Our federated learning-based AI system carries out the following tasks for each validation token:

Authorized licensed use limited to: Military Institute of Science and Technology. Downloaded on August 25,2025 at 02:48:40 UTC from IEEE Xplore. Restrictions apply.

Load historical certificate data from local nodes to ensure data privacy and maintain decentralization.

- Extract features from each node's certificate data into a comprehensive feature matrix without data centralization.
- Initialize and synchronize the federated learning model across nodes for uniformity.
- Train the federated model on feature matrices from multiple institutions, allowing the model to generalize across diverse datasets.
- Predict anomaly scores on new certificate data using the federated model.
- Flag certificates with anomaly scores above the established threshold for further review.

By decentralizing the training process through federated learning, Validify's model enhances security and privacy, minimizes data transfer, and improves the system's scalability. This collaborative approach not only identifies anomalies with high precision but also enables a scalable, secure validation process that can accommodate a growing number of institutions and certificate types, reinforcing the trustworthiness of the certification process.

E. Implementation:

a) Algorithm: create_VaLiDiFy_block procedure

add_block(tokens, account):

if chain is empty:

set previous_hash to "0"

else:

set previous_hash to the hash of the last block in the chain

create new_block with:

- current_block_id

- tokens

- previous_hash

check smart contract criteria for certificate issuance:

if account does not meet eligibility requirements:

print "Eligibility requirements not met" and return

mine new_block

validate and append new_block to the chain

end procedure

The CreateBlock algorithm outlines the process of adding a new block to the blockchain. It begins by finding the previous hash based on the existing chain state. Then, it creates a new block with all necessary attributes, such as tokens, smart contracts, and prices. This block, along with others, undergoes mining to achieve consensus within the system and is validated before being added to the chain.

b) Algorithm: Validate_VaLiDiFy_block

procedure validate_block(verification_hash)

for each block in chain:

if block.verification_hash == verification_hash:

if not block.validate_block():

print "Block data has been tampered with."

return None

return block

return None end function

The ValidateBlock algorithm is responsible for validating a block within the blockchain. It picks up a node and iterates through the entire chain. If a match is found, it checks for any tampering within the block's data. If the block is uncompromised, it returns the validated block; otherwise, it notifies the organization of data tampering.

c) Smart contract Implementation of VaLiDiFy:

class Block:

initialize block (block_id, tokens, previous_hash,

account_info)

calculate_hash(): generate hash from block contents verify_eligibility(): check eligibility using smart contract rules

class Blockchain:

initialize chain and load from database add_block(tokens, account_info): create block, check

eligibility, mine, and append to chain

validate_chain(): ensure each block's integrity in chain export_chain(): save chain to file for backup/auditing

The Smart Contract Implementation in Validify uses a proof-of-authority-based consensus mechanism, where each block is initialized with essential attributes such as ID, tokens, hash, and account information. Each block's eligibility for issuance is verified by a marking-based system within the consensus mechanism. This setup ensures data integrity, allowing for scalability and providing a secure and auditable certificate issuance process.

F. Deploying VaLiDiFy

Illustrates the deployment of the VaLiDiFy certificate validator. The figure shows the output resulting from creating and downloading individual certificates, executed through a custom blockchain framework. The verification hash acts as a unique identifier for each deployment, providing traceability. Gas consumption values are initialized and represent the computational resource costs during deployment. All data is securely stored within a cryptographic ledger on the blockchain. Below, at Fig 5, is shown the User interface of VaLiDiFy.

Fig 5: User Interface.

Authorized licensed use limited to: Military Institute of Science and Technology. Downloaded on August 25,2025 at 02:48:40 UTC from IEEE Xplore. Restrictions apply.

IV. RESULT & COMPARISON

A. *Illustration of Certificate Validation System*

Figure 6, 7 and 8 provide an illustrated result of the certificate validation system through various stages, including initial registration, entering certificate details, and validation through different verification stages. Upon registration, a user's information is verified and kept in VaLiDiFy's MongoDB database. To guarantee long-term accessibility, the personal data is then uploaded to the IPFS (InterPlanetary File System) and pinned. Data that has not been pinned will be removed by IPFS garbage collection. In a same manner, when an organization registers, its data is incremented and saved on IPFS.

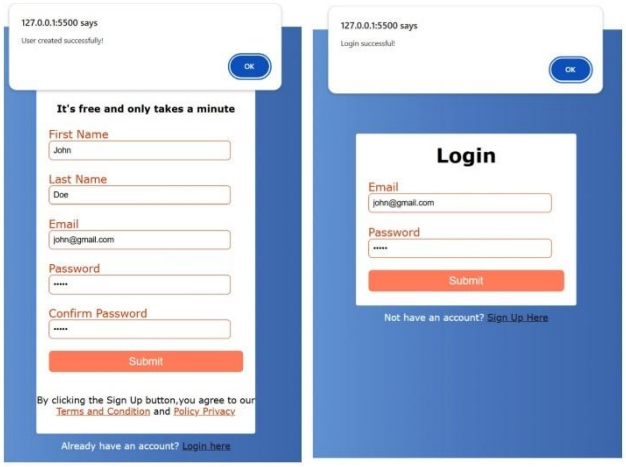

Fig 6: Initial Registration / Login

B. *Certificate Issuance*

The registered institution can submit information such as name, position, guests, and institution after the first registration stage. This information is used to issue a certificate. A verification hash, produced by passing the data across the blockchain, can be used by users to confirm the information.

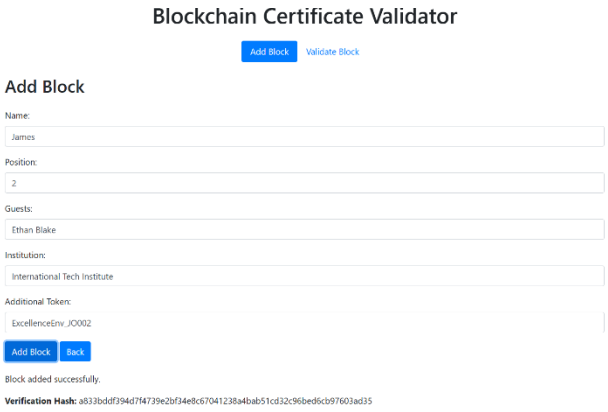

Fig 7: Certificate Issuance

C. *Verification and Validation*

The details are checked in the last phase, and all certificates that have been supplied are processed by the smart contract. The information's legitimacy is subsequently confirmed by comparing the verification hash with the blockchain record. The hash is verified following blockchain validation, offering traceability and guaranteeing the safety and security of every data.

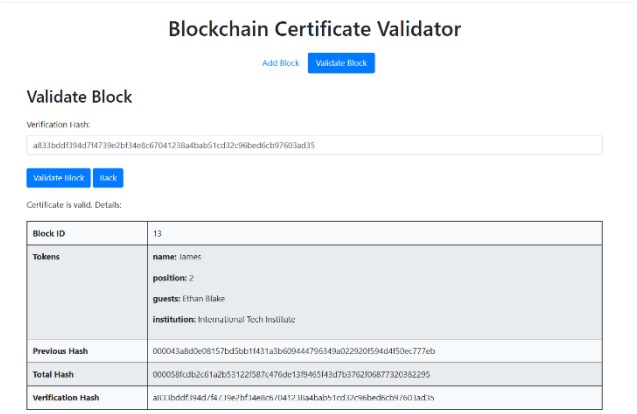

Fig. 8: Verification

D. *Comparison*

The goal of the Validify system is to provide a trustworthy, accountable, and secure certificate validation platform. It leverages a permissioned, private blockchain network instead of widely used platforms like Ethereum or Hyperledger, allowing for greater control over the system and enabling the addition of customized features. Validify enhances transparency and efficiency within its own framework. In contrast, VaLiDiFy goes beyond smart contracts by utilizing its own permissioned, privatized blockchain and integrating AI to guarantee data consistency and detect any discrepancies. ZHOU, Wang & TAO, Jun & LI, Xin (2023) [11] propose a system having multiple stakeholders, such as authorities, students, and verifiers, for allocation of credits based on performance feedback. However, VaLiDiFy ensures the highest level of data security by keeping exchange of information restricted between the Institute and VaLiDiFy exclusively, with no access for external entities. Thereby enhancing privacy without sacrificing transparency within the system. Khushal Y. Bheke, Aniket R. Misal, Nilkanth S. Pokharkar, and Prof. Gunjal T. S (2023) [6] primarily utilize Proof of Work to address double-spending and protect the decentralized ledger from attacks. In contrast, VaLiDiFy has adopted a model based on Proof of Authority (PoA) which would reduce processing costs and also improve efficiency by replacing the traditional concept of gas fees with a redefined marking-based system. This marking-based approach, governed by smart contracts, sets a specific threshold value required for certificate issuance, streamlining the process without relying on gas fees.

Furthermore, VaLiDiFy employs refracted learning, achieving approximately 94% accuracy to detect anomalies and ensure the integrity of each blockchain block during the initialization process. This AI-based layer offers an additional

Authorized licensed use limited to: Military Institute of Science and Technology. Downloaded on August 25,2025 at 02:48:40 UTC from IEEE Xplore. Restrictions apply.

safeguard against any data discrepancies throughout the validation system. Unlike the Ethereum-based system used by Jiin-Chiou Cheng, Narn-Yih Lee, Chien Chi, and Yi-Hua Chen (2018) [1], VaLiDiFy maintains a low transaction processing time for certificate issuance through its customized user interface, tailored for efficient and secure management of certificate validation processes. A comparison table for the same is provided below as fig. 9 for reference with respect to the above noted.

Parameters	Zhou, Wang & others (2023) [11]	Jiin-Chiou Cheng & others (2023) [1]	Kushal Y. Bheke & others (2023) [6]	Kushal Y. Bheke & Ankit R. and others [7]	VaLiDiFy
Blockchain Network	Ethereum Based	Ethereum Based	Hyperledger Based	Hyperledger Based	Permissioned Private Blockchain
Marking Scheme-based System	Traditional Gas Fees	Traditional Gas Fees	Traditional Gas Fees	Traditional Gas Fees	Marking Scheme Based System
AI Integration	Not Integrated	Not Integrated	Not Integrated	Not Integrated	Integrated for Robustness
Robustness	Robust	Robust	Robust	Robust	Highly Robust
Transparency	Not Transparent	Not Transparent	Not Transparent	Transparent	Consortium Based Transparency

Fig. 9: Comparison Table

V. CONCLUSION

This paper introduces a Blockchain-based certificate validation platform leveraging the network's immutability and decentralized storage via IPFS, while utilizing AI to ensure data consistency. Proof of Authority is employed, along with a marking-based smart contract system to manage costs. While popular platforms like Hyperledger and Ethereum exist, VaLiDiFy utilizes a custom permissioned, privatized blockchain to ensure transaction transparency. MongoDB and IPFS support scalable user data storage. The paper reviews existing literature, positioning VaLiDiFy as a primary approach for certificate validation. Institutes are assigned key roles to address evolving requirements. Despite challenges like blockchain complexity and the need for technical expertise, this integrated system offers efficient, secure, and scalable digital certificate management, distinguishing itself from more complex or isolated solutions in current research.

A. Future Scope

Future advancements will involve the integration of deep learning and real-time anomaly detection to enhance the accuracy of certificate validation. There will be a push for certificate formats standardization across institutions globally, which would facilitate seamless verification. The implementation of decentralized identity systems and biometric authentication will be prioritized to improve privacy and security. Additionally, adopting more energy-efficient consensus mechanisms and edge computing will support sustainable operations by being environmentally friendly. focus will also be on fostering federated AI models and explainable AI to enhance transparency in fraud detection, along with the development of mobile apps and automated retrieval systems for easier certificate management.

REFERENCES

[1] Jiin-Chiou Cheng, Narn-Yih Lee, Chien Chi and Yi-Hua Chen. (2018) Blockchain and Smart Contract for Digital Certificate. Available: DOI: 10.1109/ICASI.2018.8394455

[2] Wei Cai, Zehua Wang, Jason B. Ernst, Zhen Hong, Chen Feng and Victor C.M Leung. (2018) Decentralized Applications: The Blockchain Empowered Software System.

[3] Nitin Kumavat, Swapnil Mengade, Dishant Desai and Jesal Varolia. (April 2019) Certificate [3] Verification System Using Blockchain. International Journal for Research in Applied Science & Engineering Technology (IJRASET), (Volume 7 Issue IV).

[4] S. Sunitha kumari, D. Saveetha "Blockchain and Smart Contract for Digital Document Verification" Department of Information Technology-SRM Institute of Science and Technology.

[5] A. Gayathiri, J. Jayachitra, Dr. S. Matilda (2020), "Certificate Validation using Blockchain", IEEE International Conference on Smart Structures and Systems ICSSS, 7th Conference.

[6] Khushal Y. Bheke, Aniket R. Misal, Nilkanth S. Pokharkar, Prof. Gunjal T. S, "Digital Certificate Verification Using Blockchain Technology" (2023), International Journal of Research Publication and Reviews ISSN 2582-7421.

[7] Khushal Y. Bheke, Aniket R. Misal, Nilkanth S. Pokharkar, Prof. Gunjal T.S. (2023), "Enhancing Educational Certificate Verification with Blockchain and IPFS: A Decentralized Approach Using Hyperledger Fabric", EM Journal, ISSN 2217-8309, DOI: 10.18421/TEM124-51, 12(4).

[8] Kabashi, F., Snopçe, H., Luma L, A., Aliu, A., Shkurti, L. (2023). "Implementation of Elliptic Curve Digital Signatures in Blockchain for Management of Certificates in Higher Education", Journal of Engineering and Applied Sciences Technology, 5(2).

[9] M Manjunatha, Dr Usha J., 2023, Certificate Validation using Blockchain Technology. International Research Journal of Modernization in Engineering Technology and Science, 05(09).

[10] Neethu Gopal, Vani V Prakash, 2018, Survey on Blockchain Based Digital Certification. International Research Journal of Engineering and Technology, 05(11).

[11] ZHOU, Wang & TAO, Jun & LI, Xin. (2023). A Blockchain-Based Certificate System with Credit Self-Adjustment. Wuhan University Journal of Natural Sciences.

[12] Rai, B. K., & Srivastava, A. K. (2017). Prototype implementation of patient controlled pseudonym-based mechanism for electronic health record (PcPbEHR). Int J Res Eng IT Soc Sci Impact Factor, 6(07), 07.

[13] Rai, B. K., Kumar, G., & Balyan, V. (Eds.). (2023). AI and Blockchain in Healthcare. Singapore: Springer Nature.

[14] Rai, B. K., Sharma, P., Singhal, S., & Paruti, B. S. (2023). Decentralized Blockchain-Enabled Employee Authentication System. International Journal of Reliable and Quality E-Healthcare (IJRQEH), 12(1), 1-13. https://doi.org/10.4018/IJRQEH.323570

Authorized licensed use limited to: Military Institute of Science and Technology. Downloaded on August 25,2025 at 02:48:40 UTC from IEEE Xplore. Restrictions apply.