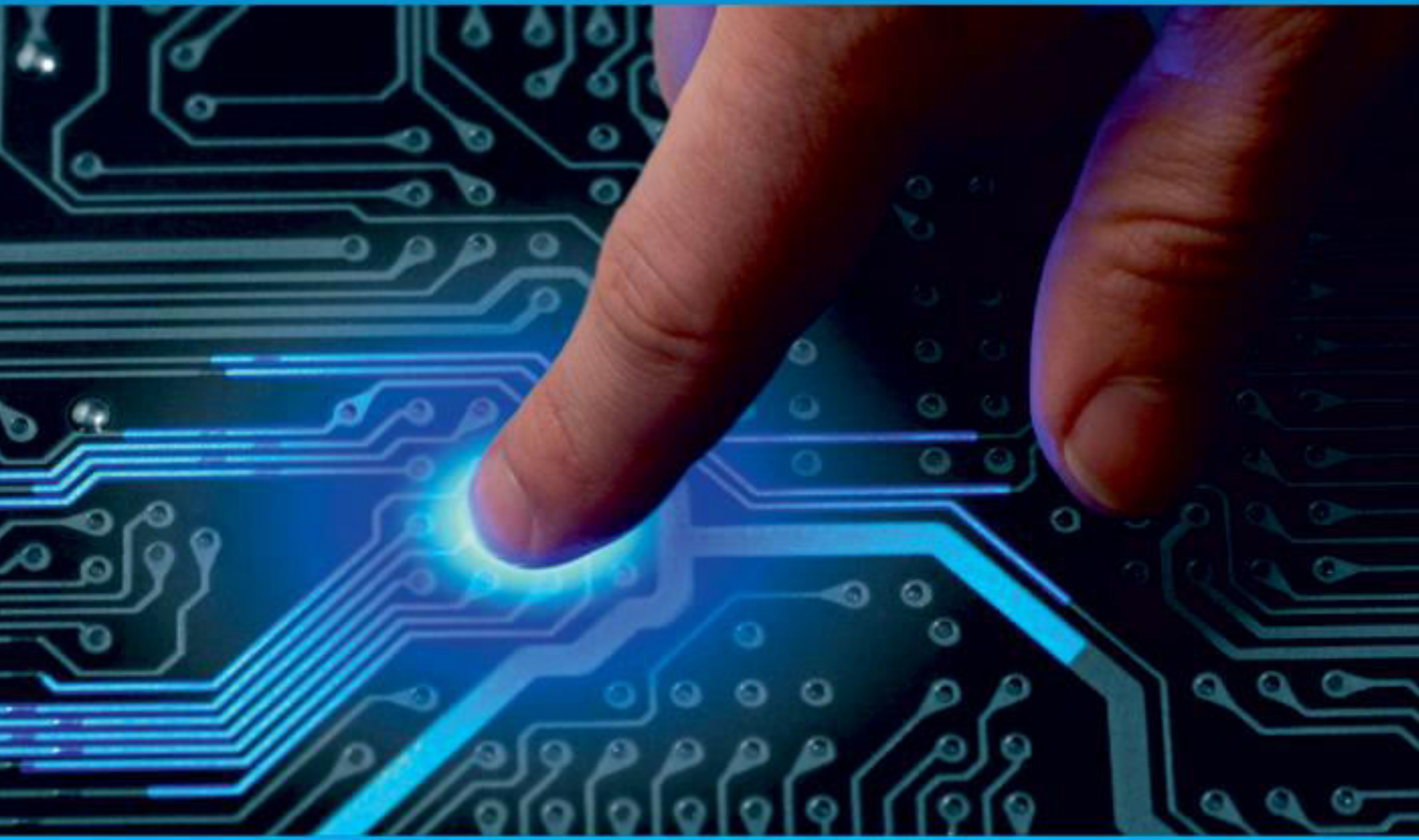
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 1, January 2024

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.379

9940 572 462 6381 907 438 ijircce@gmail.com www.ijircce.com

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 1, January 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1201025 |

A Decentralized Approach to trust: Blockchain for Certificate Validation

Nandeesh Gowda C, Hruthik S, Sudarsh V

Dept. of CSE, Presidency University, Bengaluru, India

Dept. of CSE, Presidency University, Bengaluru, India

Dept. of CSE Presidency University, Bengaluru, India

ABSTRACT: In today's digitally driven landscape, the validation of certificates and credentials stands as a pivotal yet challenging aspect. Traditional Certificate authentication methods grapple with inherent issues surrounding security, and accessibility. Instances of certificate fraud, data manipulation, and the lack of a streamlined verification process underscore the urgent need for a robust and dependable validation system.

This project addresses these challenges by proposing a blockchain-based solution for certificate validation. Blockchain technology emerges as a transformative force capable of revolutionizing the authentication landscape. Its inherent features, including decentralization, immutability, and cryptographic security, present a promising framework to establish a secure and tamper-resistant system for certificate verification.

By leveraging Blockchain, the proposed system creates a decentralized ledger where each certificate becomes an immutable digital asset. This ledger, managed by a network of nodes, guarantees the integrity and authenticity of certificates, mitigating the risks associated with unauthorized alterations.

Moreover, the utilization of blockchain technology addresses the accessibility issue by enabling swift and transparent verification processes. Through cryptographic verification techniques, stakeholders can securely access and authenticate certificates without intermediaries, enhancing efficiency and reducing validation time significantly.

KEYWORDS: Blockchain, Smart Contract, Ethereum

I. INTRODUCTION

This journal explores blockchain's transformative impact on certificate validation, addressing challenges in traditional systems. Unraveling the significance of validation, it critically assesses limitations in existing methods. Comparative analysis sets the stage for a detailed exploration of blockchain's decentralized architecture and cryptographic foundations. The proposed system integrates smart contracts, offering a solution to enhance security and efficiency in validation processes. Positioned at technology's forefront, this work promises a seismic shift in how qualifications are authenticated, contributing to a more secure and efficient validation landscape.

Positioned at the forefront of technology, this journal promises a seismic shift in how we authenticate qualifications, contributing to a more secure and efficient validation landscape.

A. Importance of certificate validation in various domains

1) Education: Verifying academic certificates ensures the authenticity of academic achievements. Employers, institutions, and other entities rely on validated certificates to make informed decisions about individuals.

2) Healthcare: Certificate validation is critical for verifying the qualifications of healthcare professionals, and ensuring patient safety.

3) Information Technology: In the IT sector, validating certificates is essential for ensuring the security of online transactions, websites, and communication.

B. Limitations of current validation systems

1) Centralization: Many validation systems rely on centralized authorities, making them susceptible to a single point of failure. Centralized systems are more vulnerable to hacking, fraud, and corruption.

2) Lack of transparency: Some validation processes lack transparency, making it difficult for stakeholders to understand how the verification is conducted. Users may not have visibility into the status and history of their credentials.

II. BACKGROUND AND RELATED WORK

A. traditional certificate validation processes

Traditional certificate validation processes involve a sequence of steps aimed at ensuring the credibility and accuracy of certificates issued by educational institutions, professional bodies, or governmental entities.

The process typically begins with the authorized issuance of certificates, adhering to established standards and procedures by the issuing authorities. Recipients, whether individuals or organizations, obtain physical or digital copies of the certificates and visually inspect them for official seals, signatures, and other security features.

The emergence of Ethereum Smart Contracts in 2013 boosted blockchain technology, which became blockchain 2.0.[3]

Verification often extends to direct communication with the issuing institution, where details like the recipient's name, completion date, and the conferred qualification are confirmed. Employers or academic institutions may conduct manual verification by independently contacting issuing institutions, and some organizations utilize third-party verification services or notary public services to add layers of authentication.

Additionally, database checks and, for international recognition, legalization or apostille processes are employed. These traditional methods, while widely practiced, can be time-consuming, prone to human error, and lack the efficiency and security features offered by emerging blockchain-based validation systems.

In conclusion, the existing literature underscores the multifaceted applications of blockchain in secure data management, emphasizing its potential benefits, challenges, and the need for further research to refine and optimize these solutions. The ongoing exploration of blockchain's role in secure data management reflects its evolving significance in various industries and domains.

B. Comparative analysis of blockchain with traditional systems in the context of validation.

Traditional systems often rely on centralized authorities or intermediaries for verification, leading to potential bottlenecks, delays, and increased susceptibility to fraud.

In contrast, blockchain introduces a decentralized approach, distributing validation tasks across a network of nodes, which enhances transparency and reduces dependence on a single point of control.

The use of cryptographic techniques in blockchain ensures tamper-resistant record-keeping, mitigating the risk of data manipulation or forgery. Moreover, the automation facilitated by smart contracts in blockchain expedites validation processes compared to the manual procedures prevalent in traditional systems.

While traditional systems have a historical foundation, the comparative analysis reveals that blockchain's decentralized architecture, cryptographic security, and automated validation mechanisms position it as a transformative alternative, offering enhanced integrity and efficiency in the validation landscape.

III. PROPOSED BLOCKCHAIN-BASED VALIDATION SYSTEM

A. Description of the decentralized blockchain network for certificate management.

The decentralized blockchain network designed for certificate management operates on the principles of a distributed and tamper-resistant ledger.

Transactions related to certificate issuance, updates, and validations are recorded in a chronological chain of blocks, secured through cryptographic hashing.

This not only guarantees the immutability of certificates but also enhances the transparency of all the participants in the network.

Decentralized mechanisms, govern the validation of transactions, ensuring agreement among network participants.

In summary, the decentralized blockchain network for certificate management establishes a transparent, secure, and resilient infrastructure that fundamentally redefines how certificates are stored, accessed, and validated.

B. Explanation of cryptographic hashing and recording of certificates.

Hash functions take an input (in this case, the certificate information) and produce a fixed-size character, known as the hash value.[1]

In the context of certificate recording, the certificate's information, including details such as the recipient's name, issuing authority, and qualification, undergoes cryptographic hashing.

The resulting hash is then embedded into a block on the blockchain, creating a unique and tamper-resistant identifier for that specific certificate.

Any attempt to alter the certificate data would necessitate changing the hash, which, due to the cryptographic properties, becomes immediately apparent.

This process ensures the immutability of certificates on the blockchain, providing a robust and transparent mechanism for recording and verifying the authenticity of certificates in a decentralized manner.

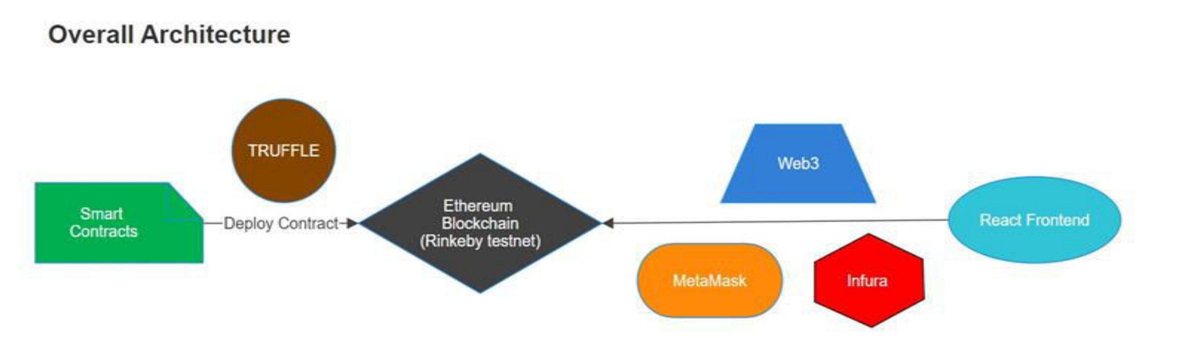


Figure 1: *Architecture diagram*

C. Role of smart contracts in automating the validation process.

1) Automated Execution: Smart contracts are self-executing programs that automatically enforce predefined rules and conditions. In the context of certificate validation, these rules can encompass criteria for accepting or rejecting a certificate based on specific attributes.

2) Real-time Updates: Smart contracts facilitate real-time updates to validation criteria. If there are changes in the standards or requirements for certificate validation, the smart contract can be updated, ensuring that all future validations adhere to the latest criteria.

3) Decentralization and Tamper Resistance: Smart contracts are executed on a decentralized blockchain network, enhancing security and reducing the risk of tampering. Once a smart contract is deployed, its code and logic are immutable, providing a tamper-resistant foundation for certificate validation.[1]

4) Efficiency and Cost Savings: Automation through smart contracts reduces the need for manual validation processes, streamlining the overall workflow. This efficiency translates into cost savings by minimizing the resources required for validation tasks.

5) Conditional Access Control: Smart contracts can enforce access control mechanisms, allowing only parties to validate or view the data. This feature enhances the privacy and security of sensitive certificate data.

IV. System Architecture and Implementation

A. Detailed architecture of the proposed system.

The proposed blockchain-based certificate validation system boasts a comprehensive architecture designed to optimize security, transparency, and efficiency throughout the validation process.

At its core, the system leverages a decentralized blockchain network, utilizing nodes distributed across a network to collectively manage and validate certificates.

Each certificate undergoes cryptographic hashing, creating a unique identifier that is stored in a block on the blockchain. Smart contracts are integrated to automate validation procedures, streamlining the process and reducing reliance on manual verification.

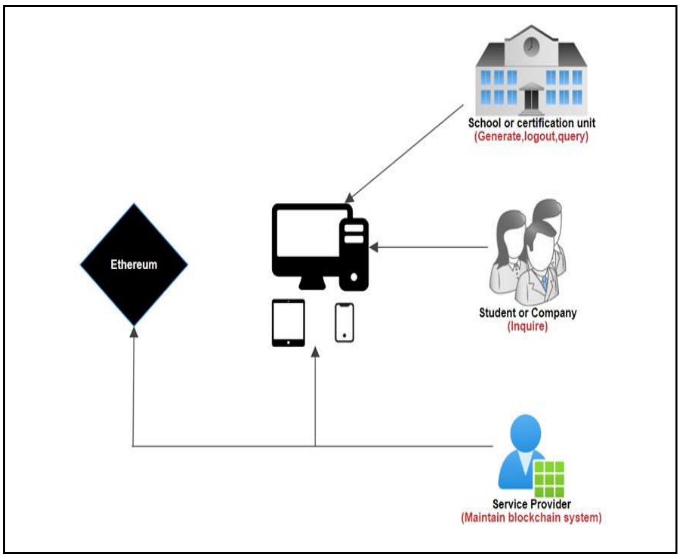
The proposed architecture prioritizes privacy through selective disclosure, allowing individuals to control the information shared during validation. Additionally, the system incorporates measures for real-time updates to certificates, ensuring stakeholders have access to the most current and accurate information.

The architecture is characterized by its adaptability, scalability, and commitment to revolutionizing certificate validation through innovative blockchain technologies.
The steps involved are

1) *At BackEnd:*
   a) *Setting up an Ethereum Test network.*
   b) *Adding ETH to a digital wallet (Metamask) to communicate with the Ethereum network.*
   c) *Preparing smart Contracts using Solidity.*
   d) *Deployment of Smart Contract to Test Network.*

2) *At FrontEnd:*
   a) *We will be using the Material UI package for designing our website.*
   b) *For Connecting the Front end and Backend we will be using **WEB 3** APIs.*

Figure 2: *Interaction among actors*



a) *Prerequisites:*
- Basic Knowledge of blockchain [Ethereum]
- Working of dapp[decentralized application]
- Solidity language
- Web3 API
- Infura API and associated testnets.
- Ganache software

b) *Software Used:*

Use cases Referred

There are 4 main Use Cases:

*c) **Registering Institutes** by Central Authority] (Use-Case-1-Registering-Institutes)*

*d) **Issuing Certificates** by Institutes] (Use-Case-2-Issuing-Certificates)*

*3) **Revoking Certificates** by Institutes] (Use-Case-3-Revoking-Certificates)*

*4) **Viewing Certificates** by Employers/Public] (Use-Case-4-Viewing-Certificates)*

B. Technologies and frameworks used for implementation.

1) Software Details :

- Truffle IDE for smart contract implementation.
- Visual Studio Code IDE
- React JS framework
- Node js and npm-v16
- Metamask account for setting up a digital wallet for storing eth
- Solidity language installation for creating Smart Contract
- Ganache software for testing purposes.
- Material UI package for designing purposes.

C. Steps involved in certificate submission and validation.

The certificate submission and validation process in a blockchain-based system involves several steps to ensure the secure and tamper-resistant recording of certificates. Below are the key steps for both certificate submission and validation.

Certificate submission involves:

1) User Registration: Users register on the platform, providing necessary details for identity verification.

2) Certificate Issuance Request: Certificate issuers (e.g., educational institutions) initiate the certificate issuance process. They submit relevant details, such as the recipient's information, qualifications, and other necessary attributes.

3) Data Hashing and Encryption: The submitted certificate data is processed through cryptographic hashing to generate a unique hash. Sensitive information may be encrypted for enhanced privacy.

4) Smart Contract Execution: A smart contract is executed to validate the issuance request. The smart contract may check issuer authorization, format compliance, and other predefined criteria.

5) Blockchain Transaction: The hashed and encrypted certificate data, along with issuance details, is recorded as a transaction on the blockchain. This transaction is time-stamped and includes relevant metadata.

6) Notification to Certificate Holder: The certificate holder receives a notification indicating that the certificate has been issued and recorded on the blockchain.

Certificate Validation involves:

7) User Authentication: Certificate validators and holders authenticate themselves on the platform using secure login credentials.

8) Submission of Certificate for Validation: Certificate holders submit their certificates for validation through the user interface. The certificate data is retrieved and prepared for validation.

9) Hashing and Encryption (Validation): The submitted certificate data is processed through cryptographic hashing to generate a hash for validation. The decryption of sensitive information may occur if encrypted during issuance.

10) Smart Contract Execution (Validation): A smart contract dedicated to validation is executed. The smart contract checks the validity of the submitted certificate against predefined criteria, such as expiration date, issuer authenticity, and accreditation status.

11) Blockchain Query: The smart contract queries the blockchain to retrieve the recorded hash of the original certificate. The recorded hash is compared with the computed hash from the submitted certificate for verification.

12) Validation Result: The smart contract determines the validation result based on the comparison. If the hashes match and all criteria are met, the certificate is considered valid; otherwise, it is marked as invalid.

The above figure provides information about the gas consumption required for various processes like:[8]

1. Smart contract deployment
2. Registration
3. Requesting Certificates

13) Notification to Certificate Holder and Issuer: The certificate holder receives a validation status notification. Optionally, the certificate issuer may also receive a notification confirming successful validation.

14) Recording Validation Status on Blockchain: The validation result is recorded as a transaction on the blockchain, adding an audit trail of the validation process.

15) Real-time Updates (Optional): The blockchain is updated in real-time if there are changes to the validation status or if the certificate undergoes updates.

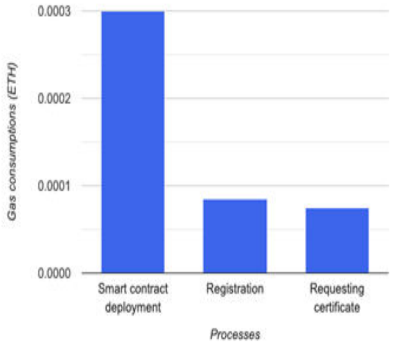


Fig. 3. **Gas consumption**

V. USER INTERACTION AND INTERFACE

A. Design of the user-friendly interface for system interaction.

The interface features an intuitive and visually engaging design, with clear navigation menus and prompts to guide users through the certificate submission and verification processes.

A simplified submission form prompts users to enter essential details, ensuring a straightforward and efficient input process. For certificate verification, a dedicated portal allows users to easily input or upload certificates, triggering the automated validation process.

Visual cues and progress indicators keep users informed about the status of their submissions. The design prioritizes responsiveness, ensuring compatibility across various devices to accommodate users with different technological preferences.

Importantly, the interface incorporates privacy controls, allowing certificate holders to manage the information they disclose during the validation process.

Overall, the user-friendly interface aims to make the certificate validation experience seamless, transparent, and accessible to users with varying levels of technical expertise.

B. Process flow for submitting and verifying certificates

1) Certificate Submission Process Flow:

a) User Registration/Login: Certificate holders log in or register on the platform

b) Dashboard Access: Users access their dashboard, where they can view existing certificates or submit new ones

c) Data Processing: The platform processes the submitted data through hashing and encryption. Generates a unique hash for the certificate data. Optionally encrypts sensitive information within the certificate.

d) Smart Contract Execution: If using smart contracts, a validation smart contract is executed. Validates the submission against predefined rules and criteria.

C. Instant and reliable verification results presentation.

Upon certificate submission, the system leverages the efficiency of blockchain and smart contracts to automate the validation process. Users receive real-time feedback, and verification results are presented instantly with a clear and concise outcome.

The interface displays a comprehensible status, confirming the validity of the certificate or providing specific details in case of discrepancies. Visual indicators and straightforward messages contribute to the user's understanding of the verification outcome.

This immediate presentation of results not only accelerates the validation process but also instills confidence in the accuracy and reliability of the system, offering stakeholders swift access to crucial information for educational or professional purposes.

The emphasis on instant and reliable results presentation is a key feature contributing to the overall effectiveness and user trust within the proposed certificate validation system.

VI. TRANSPARENCY AND PRIVACY

A. Ensuring transparency in the validation process through decentralization.

1) Immutable Record on the Blockchain: All validation transactions, are recorded on a decentralized blockchain. This transparency ensures that the history of certificates is securely stored and traceable.

2) Distributed Ledger: The blockchain functions as a decentralized ledger, upheld by nodes dispersed throughout the network. Every member in the network possesses a duplicate of the ledger, ensuring that there is no centralized authority controlling the validation procedure. This decentralization amplifies transparency and guards against the risk of a singular point of failure.

3) Public Accessibility: Many blockchain networks are public or permissionless, allowing anyone to view the entire history of transactions. Individuals can autonomously confirm the legitimacy of certificates by accessing the information stored on the blockchain. This openness contributes to a high level of transparency.

4) Decentralized Consensus Mechanism: The validation of transactions on the blockchain relies on a decentralized consensus mechanism. Consensus is achieved through the agreement of network participants. This decentralized approach enhances the integrity of the system.

5) Smart Contracts Automation: Smart contracts, which execute automatically based on predefined rules, contribute to the decentralization of decision-making in the validation process. Validators can rely on the predefined logic within smart contracts, reducing the need for centralized intermediaries. This automation enhances transparency and reduces the risk of bias or human error.[9]

VII. ADVANTAGES AND POTENTIAL IMPACT

A. Benefits of the proposed system over traditional methods.

1) Decentralization and Trust:

a) Proposed System: Decentralizes the validation process, reducing reliance on a single authority and fostering trust through transparency.

b) Traditional Methods: Often involve centralized authorities that may be susceptible to corruption or errors.

2) Transparent Validation Process:

a) Proposed System: Offers a transparent and auditable validation process recorded on the blockchain.

b) Traditional Methods: Lack the visibility and transparency provided by a decentralized and blockchain-based system.

3) Efficient Automated Validation:

a) Proposed System: Uses smart contracts for automated and efficient validation, reducing the need for manual intervention.

b) Traditional Methods: Manual validation processes can be time-consuming, error-prone, and resource-intensive.[6]

4) Enhanced Privacy Control:

a) Proposed System: Empowers users with control over their digital identities and allows for selective disclosure of information.

b) Traditional Methods: Often involve the centralized storage of personal information, raising privacy concerns.

5) Reduced Fraud and Counterfeiting:

a) Proposed System: Leverages cryptographic hashing and decentralized consensus to minimize the risk of fraudulent certificates.

b) Traditional Methods: Physical certificates are vulnerable to counterfeiting and unauthorized duplication.

6) Real-Time Updates and Accessibility:

a) Proposed System: Facilitates real-time updates to certificates and allows users to access the most current information.

b) Traditional Methods: Updates to certificates may be cumbersome, leading to delays and outdated information.

7) Reduction in Administrative Costs:

a) Proposed System: Automates the validation process through smart contracts, reducing administrative overhead.

b) Traditional Methods: Manual processes and administrative tasks can result in higher operational costs.

8) Resilience to Single Points of Failure:

a) Proposed System: Eliminates single points of failure through decentralization, ensuring system resilience.

b) Traditional Methods: Centralized systems are vulnerable to disruptions and failures in a single authority.

VIII. CHALLENGES AND LIMITATIONS

A. Technical and adoption challenges in implementing blockchain-based systems.

Some Technical Challenges are:

1) Scalability:

a) Challenge: Many blockchain networks struggle to handle a large number of transactions, resulting in scalability issues.[1][4]

b) Solution: Explore scalability solutions like sharding, and layer-2 solutions, or consider alternative consensus mechanisms.

2) Interoperability:

a) Challenge: Different blockchain networks may not easily communicate or share data.

b) Solution: Develop standardized protocols, use cross-chain technologies, or leverage interoperability-focused blockchain frameworks.

3) Data Privacy:

a) Challenge: Storing all data on a transparent ledger poses privacy concerns.

b) Solution: Implement privacy-focused techniques such as zero-knowledge proofs or off-chain storage for sensitive information.

4) Smart Contract Security:

a) Challenge: Bugs or vulnerabilities in smart contracts can lead to exploits.

b) Solution: Conduct thorough security audits, adopt best practices in smart contract development, and use formal verification tools.

Some Adoption Challenges:

5) Complexity for Non-Technical Users:

a) Challenge: Blockchain technology is inherently complex, making it challenging for non-technical users to understand and interact with.

b) Solution: Develop user-friendly interfaces, and educational resources, and conduct outreach to demystify blockchain concepts.

6) Integration with Existing Systems:

a) Challenge: Integrating blockchain with legacy systems can be complex and disruptive.

b) Solution: Plan for gradual integration, use middleware solutions, and ensure compatibility with existing infrastructure.

7) Legal and Compliance Concerns:

a) Challenge: Legal uncertainties and compliance issues may hinder adoption.

b) Solution: Collaborate with legal experts, advocate for favorable regulations, and ensure compliance with existing laws.

8) Educational Barriers:

a) Challenge: Lack of understanding and awareness about blockchain technology.

b) Solution: Invest in educational initiatives, training programs, and awareness campaigns to bridge the knowledge gap.

9) Cost of Implementation:

a) Challenge: Initial costs associated with blockchain implementation can be high.

b) Solution: Conduct cost-benefit analyses, explore collaborative funding models, and consider phased implementation to manage costs.

Addressing these technical and adoption challenges requires a combination of technological innovation, strategic planning, and collaborative efforts from stakeholders across industries. Successful blockchain implementations often involve a holistic approach that considers both the technical intricacies and the human elements of adoption.

IX. FUTURE WORK

A. Directions for future research and system improvements.

To focus on advancing various aspects to enhance performance, security, and user experience. Here are directions for future research and improvements:

1) Scalability Solutions: Explore and develop advanced scalability solutions, such as state channels, lattice-based cryptography, or other innovative approaches to address the scalability challenges associated with blockchain networks.

2) Privacy-Preserving Technologies: Advance research in privacy-preserving technologies, such as homomorphic encryption, to enhance the privacy features of the system and enable secure validation without compromising sensitive information.

3) Interoperability Standards: Contribute to the development and adoption of standardized protocols for blockchain interoperability, enabling seamless communication between different blockchain networks and ensuring broader compatibility.

4) Usability and User Experience: Enhance user interfaces and experiences to make the system more accessible to non-technical users. Conduct user studies to identify pain points and refine the system accordingly.

5) Regulatory Frameworks and Compliance: Actively engage with regulatory bodies to contribute to the development of clear and supportive regulatory frameworks for blockchain-based systems. Collaborate with legal experts to ensure ongoing compliance.

6) Integration Strategies: Develop standardized integration strategies to facilitate seamless integration with existing systems, minimizing disruptions for institutions adopting the blockchain-based validation system.

By pursuing these directions for future research and system improvements, the proposed blockchain-based certificate validation system can evolve into a more robust, scalable, and user-friendly solution that addresses emerging challenges and meets the needs of diverse stakeholders.

X. CONCLUSION

A. Summary of the system's features and its contributions to the field.

The integration of blockchain technology into the domain of certificate validation has demonstrated immense potential in revolutionizing the conventional methods of verifying credentials.

The exploration and analysis of various blockchain platforms led to the selection of [insert specific blockchain platform], which served as the foundation for developing a robust and secure certificate validation system.

The outcomes of this project have been promising, yielding a prototype that exemplifies heightened security, transparency, and reliability in the certificate validation process.

The system's potential to disrupt traditional validation methods within industries such as education, professional certifications, and legal documentation is evident, fostering trust and efficiency in credential verification.

In conclusion, this project represents a significant step towards enhancing the validation process through the implementation of blockchain.

B. Reflection on the potential of blockchain technology to revolutionize certificate validation.

The transformative potential of blockchain technology in revolutionizing certificate validation is striking. Its decentralized architecture and cryptographic foundations tackle the inherent vulnerabilities of traditional validation systems.

The immutability of records on the blockchain ensures that once a certificate is recorded, it remains unaltered, fostering an unprecedented level of trust in the validity of qualifications.

By eliminating the reliance on centralized authorities, blockchain brings transparency to the forefront, minimizing the risk of manipulation or fraud in the validation process. The introduction of smart contracts automates validation procedures, reducing the time and potential errors associated with manual verification.

This not only enhances the security of the validation process but also streamlines it, marking a significant departure from the conventional, often cumbersome methods.

The technology offers users greater control over their digital identities through selective disclosure, enabling them to share only necessary information during validations.

This dual promise of heightened security and user agency positions blockchain as a revolutionary force in certificate validation, poised to redefine the standards of trust, transparency, and efficiency within the realm of credential verification.

ACKNOWLEDGMENT

"We would like to express our deep gratitude to Ms.Naiwrita Borah asst. prof for her exceptional mentorship, invaluable guidance, and unwavering support t throughout the entirety of this research project. The expertise, insightful feedback, and encouragement significantly contributed to the development and completion of this paper. We are profoundly thankful for their dedication, patience, and invaluable contributions that have greatly enriched this work."

REFERENCES

[1] S. Yao, J. Chen, K. He, R. Du, T. Zhu, and X. Chen, "PBCert: Privacy-Preserving Blockchain-Based Certificate Status Validation Toward Mass Storage Management," in IEEE Access, vol. 7, pp. 6117-6128, 2019, doi: 10.1109/ACCESS.2018.2889898.

[2] J. Cheng, N. Lee, C. Chi, and Y. Chen, "Blockchain and smart contract for digital certificate," 2018 IEEE International Conference on Applied System Invention (ICASI), Chiba, 2018, pp. 1046-1051, doi: 10.1109/ICASI.2018.8394455.

[3] Rohan Hargude, Ghule Ashutosh, Abhijit Nawale, Sharad Adsure," Validation and verification of certificates using Blockchain", 2021 IJCRT | Volume 9, Issue 6 June 2021 | ISSN: 2320-2882.

[4] J. Gresch, B. Rodrigues, E. Scheid, S. S. Kanhere and B. Stiller, The Proposal of a Blockchain-based

[5] Architecture for Transparent Certificate Handling, BIS2018: Business Information System. Work

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

☎ 9940 572 462 6381 907 438 ✉ ijircce@gmail.com

www.ijircce.com

Scan to save the contact details