

BlockchainValid: A Novel Framework for Certification Validation using Blockchain and IoT Devices

Dr. Dinesh Chandra¹, Dr. S. S. Aravinth², Ravuri Ganesh Sharma³, Pupala saikumar⁴, Konduri Roshni Bala⁵ and Mallampati Bhavana⁶

¹⁻⁶Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur, Andhra Pradesh, India

Email: dinesh.pancharia@gmail.com, aravinthkrithick@gmail.com, 2100030960cseh@gmail.com, 2100032358cseh@gmail.com, 2100030690cseh@gmail.com, 2100030320cseh@gmail.com

Abstract—This paper presents a novel framework for certificate validation leveraging Blockchain technology and IoT devices. Through a comprehensive survey of existing research papers focusing on the integration of Blockchain and IoT devices, we analyze the advantages and disadvantages of these approaches. Our framework aims to address the challenges associated with certificate validation, such as reliability, security, and efficiency. By combining the immutability and transparency of Blockchain with the real-time data collection capabilities of IoT devices, our proposed solution offers a robust and trustworthy method for certificate validation in various domains. We discuss the key features of our framework, including its ability to ensure authenticity, prevent tampering, and streamline the validation process. Additionally, we highlight potential areas for future research and development in this field.

Index Terms— component, formatting, style, styling, insert.

I. INTRODUCTION

In the contemporary digital landscape, the validation of certificates stands as a pivotal process to uphold the trustworthiness and integrity of digital credentials, spanning realms such as academia, employment, and professional accreditation. With the rapid evolution of technology, there arises an imperative for validation methodologies that are not only robust but also adaptable to the dynamic digital environment.

In this research pursuit, we embark on an exhaustive exploration of various methodologies employed for certificate validation. Our investigation encompasses a broad spectrum of approaches, including blockchain-based validation, Public Key Infrastructure (PKI), hash algorithms, and the integration of blockchain with Internet of Things (IoT) devices. Their responsibility entails aiding in the implementation of various security requirements and bolstering the confidence of buyers in these systems[1].

Each methodology presents distinct strategies, drawing upon diverse technological frameworks and cryptographic principles. Through meticulous comparative analysis, we endeavor to unveil the strengths, weaknesses, and real-world applicability of these methodologies. By illuminating their unique attributes and potential challenges, our research aims to provide valuable insights to stakeholders involved in the design and deployment of certificate validation systems, facilitating informed decision-making and fostering advancements in digital credentialing practices.

II. LITERATURE SURVEY

The literature survey encompasses an exploration of various methodologies employed for certificate validation, spanning traditional approaches such as Public Key Infrastructure (PKI) and hash algorithms, as well as emerging technologies like blockchain and the integration of blockchain with Internet of Things (IoT) devices.

Emerging as a promising technology, blockchain presents a robust solution for addressing issues related to data transparency and reliability. Blockchain is defined as a distributed database that shares and stores all verified transaction records across a network of participants through a sequential chain of blocks[2].

Blockchain is an unalterable ledger of transactions established across a distributed network of peer nodes. These nodes uphold a copy of the ledger, applying transactions that have been previously authenticated through a consensus protocol. These transactions are grouped into blocks, each block cryptographically linked to the preceding one through a hash function [3].

A thorough examination of scholarly works and research contributions reveals a diverse landscape of studies focused on understanding the strengths, limitations, and practical applications of these methodologies..

Blockchain-based certificate validation has gained significant attention for its decentralized and immutable nature, with researchers investigating its security, scalability, and real-world implementations. PKI, as a cornerstone in digital certificate management, continues to be a subject of study, with advancements in cryptographic techniques aimed at addressing emerging security challenges.

The blockchain serves as an immutable transaction ledger, operating across a distributed network of peer nodes. These nodes maintain copies of the ledger, executing transactions verified through a consensus protocol. Transactions are organized into blocks, with each block cryptographically connected to the previous one through a hash function[4].

In an era characterized by digital transformation and technological innovation, the validation of academic credentials holds paramount importance in ensuring the integrity and trustworthiness of educational achievements. Traditional methods of certificate validation have often been plagued by challenges such as fraud, tampering, and inefficiency, necessitating the exploration of novel approaches to address these issues effectively.

"IoT Security Certifications: Challenges and potential approaches" could delve into specific challenges faced by IoT security certifications, such as the diverse nature of IoT devices, lack of standardized protocols, and the dynamic threat landscape. Additionally, the paper may discuss the importance of regulatory frameworks like the EU's Cyber Security Act in providing a structured approach to IoT security certification. It might explore examples of existing certification schemes and their effectiveness in addressing IoT security concerns, along with potential strategies for enhancing certification processes to better mitigate evolving threats.

In the case of "A blockchain-based framework for carbon management towards construction material and production certification," further details could include how blockchain technology ensures transparency and immutability of carbon-related data throughout the supply chain. The paper might elaborate on the role of smart contracts in automating verification processes and ensuring compliance with carbon management standards. Additionally, it could discuss the potential environmental and economic benefits of adopting blockchain-based solutions in the construction industry, such as reduced carbon emissions and improved resource efficiency.

"Blockchain-based refurbishment certification system for enhancing the circular economy" may elaborate on the specific features of the proposed certification tool, such as its ability to track the origin and history of refurbished products using blockchain technology. The paper could discuss how Hyperledger Fabric and GPS integration ensure the integrity and reliability of lifecycle information, thereby fostering consumer trust in circular economy initiatives. Furthermore, it might highlight the potential impact of blockchain-based refurbishment certification on reducing waste and promoting sustainable consumption practices.

Regarding "The Decentralized Smart Contract Certification System Utilizing Ethereum Blockchain Technology," additional information could include the technical architecture of the Ethereum-based certification system and its implementation in real-world scenarios. The paper might discuss the advantages of decentralization and autonomy offered by smart contracts in certifying student achievements, along with potential challenges such as scalability and interoperability. Furthermore, it could explore the implications of blockchain-based certification for academic accreditation processes and the recognition of student accomplishments.

"A unique secure multimodal biometrics-based user anonymous authenticated key management protocol based on blockchain mechanism" could provide further insights into the design and functionality of the proposed authentication scheme. The paper might detail the integration of hybrid MBO and dynamic template matching techniques to enhance the security and reliability of user authentication in IoT networks. Additionally, it could

discuss the potential applications of the protocol in securing access to sensitive IoT devices and networks, along with its resilience against common attack vectors.

In the case of "Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain," additional information could include the specific challenges faced by digital healthcare systems, such as data privacy concerns and the risk of tampering or unauthorized access. The paper might elaborate on the design principles of the blockchain-based application, such as its use of cryptographic techniques to ensure data integrity and confidentiality. Furthermore, it could discuss the potential impact of blockchain technology on streamlining administrative processes and improving patient outcomes in digital healthcare environments.

"Improved blockchain system for highly secured IoT integrated supply chain" may delve into the technical architecture of Trust Chain and its integration with existing supply chain management systems. The paper could discuss how consortium blockchain ensures data transparency and accountability among supply chain participants, while IoT devices facilitate real-time tracking and monitoring of product lifecycle data. Additionally, it might explore the potential scalability and interoperability challenges associated with deploying blockchain-based solutions in large-scale supply chain networks, along with strategies for mitigating such risks.

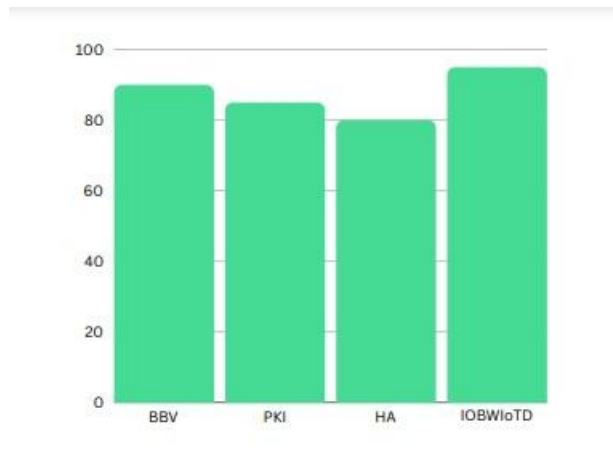


Fig1. Accuracy of the 4 methodologies in Bar graph

III. PROPOSED WORK

A. Blockchain-Based Validation

Blockchain-based validation employs the decentralized and immutable characteristics of blockchain technology to enhance the security and integrity of digital certificates. At its core, blockchain is a distributed ledger that records transactions across multiple computers in such a way that the registered transactions cannot be altered retroactively. This inherent security feature makes blockchain a powerful tool for certificate validation. When a digital certificate is issued, its details are encoded into a transaction and recorded in a block on the blockchain. This block is then linked to the previous block through a cryptographic hash, forming a chain of blocks that grows over time. Each block contains a unique hash of the previous block, a timestamp, and the transaction data, making the blockchain a secure and chronological record of transactions. Because the blockchain is distributed across a network of nodes, no single entity has control over the entire chain, enhancing its security and resilience.

For certificate validation, blockchain provides a transparent and tamper-proof mechanism. Each certificate is associated with a unique hash value generated from its data using a secure hashing algorithm, such as SHA-256. This hash is stored on the blockchain, ensuring its immutability and availability. To validate a certificate, a verifier retrieves the certificate's hash from the blockchain and compares it with the hash of the presented certificate data. If the two hashes match, it confirms that the certificate is authentic and has not been altered since its issuance. This process ensures data integrity and prevents forgery or unauthorized modifications.

Blockchain technology also offers a high level of transparency. The blockchain is publicly accessible, allowing anyone with the necessary permissions to verify the authenticity of a certificate without relying on a central authority. This decentralized approach significantly reduces the risk of fraud and increases trust among users. Additionally, blockchain's immutable nature provides a reliable audit trail, making it an excellent tool for regulatory compliance and accountability.

In practice, blockchain-based certificate validation can be applied in various domains. For example, in the education sector, academic institutions can issue diplomas and certificates on a blockchain, ensuring their authenticity and preventing falsification. Employers can easily verify the credentials of job applicants by checking the blockchain, streamlining the hiring process and enhancing trust. Similarly, in the supply chain industry, blockchain can be used to validate the certificates of origin and quality of goods, ensuring transparency and authenticity throughout the supply chain.

Moreover, blockchain's decentralized nature ensures that even if part of the network is compromised, the integrity of the certificate data remains intact. This robustness makes blockchain an ideal solution for environments that require high levels of security and trust, such as financial services, healthcare, and government services. By eliminating the need for intermediaries and providing a transparent and secure method for certificate validation, blockchain technology can significantly enhance the security and efficiency of digital transactions and communications.

Overall, blockchain-based validation represents a significant advancement in the field of digital security. Its decentralized, transparent, and tamper-proof nature provides a robust framework for ensuring the authenticity and integrity of digital certificates, making it an invaluable tool for a wide range of applications.

B. Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) is a robust and widely used framework for securing digital communications and validating certificates. It relies on asymmetric cryptography, where a pair of keys—public and private keys—are used to encrypt and decrypt data. PKI encompasses a set of roles, policies, hardware, software, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.

In a PKI system, digital certificates are issued by trusted entities known as Certificate Authorities (CAs). A digital certificate binds a public key with the identity of its holder, providing a way to verify that a public key belongs to a particular entity. When a CA issues a certificate, it digitally signs the certificate with its private key, creating a secure association between the public key and the entity's identity.

To validate a certificate in a PKI system, several steps are involved. First, the verifier obtains the certificate and checks the CA's digital signature using the CA's public key. This step confirms that the certificate was issued by a trusted CA and has not been altered. Next, the verifier checks the certificate's validity period to ensure it has not expired. The certificate includes a start date and an end date, and it is only considered valid within this time frame.

Additionally, the verifier may consult a Certificate Revocation List (CRL) or an Online Certificate Status Protocol (OCSP) responder to check if the certificate has been revoked. A CRL is a list of certificates that have been revoked by the CA before their expiration date, while an OCSP responder provides real-time status information about the certificate. These mechanisms ensure that the certificate is still valid and trustworthy.

PKI is used in a wide range of applications to secure communications and validate identities. For instance, SSL/TLS protocols, which secure web communications, rely on PKI to authenticate the identities of websites and encrypt data transmitted between the client and server. Email security protocols like S/MIME use PKI to encrypt and digitally sign emails, ensuring that the messages are confidential and authentic. Digital signatures, which provide a way to verify the authenticity and integrity of digital documents, also rely on PKI.

One of the key strengths of PKI is its hierarchical trust model. In this model, a root CA is at the top of the hierarchy, with subordinate CAs below it. The root CA's public key is widely trusted and distributed, and it signs the public keys of subordinate CAs. Subordinate CAs, in turn, issue certificates to end entities. This hierarchy allows for scalable and flexible management of digital identities. Even if a subordinate CA is compromised, the root CA can revoke its trust, maintaining the overall security of the system.

PKI also provides mechanisms for key management, including key generation, distribution, storage, and revocation. Secure key management is critical to the effectiveness of PKI, ensuring that private keys are protected from unauthorized access and that public keys are reliably distributed.

In summary, PKI is a comprehensive framework for securing digital communications and validating certificates. Its reliance on asymmetric cryptography and trusted certificate authorities provides a robust method for establishing and verifying digital identities, making it a cornerstone of modern cybersecurity.

C. Hash Algorithms

Hash algorithms are fundamental cryptographic functions that play a crucial role in ensuring the integrity and authenticity of digital data, including certificates. A hash algorithm takes an input (or "message") and returns a fixed-size string of characters, which typically appears as a sequence of numbers and letters. This output, known

as a hash value or digest, is unique to the specific input data. Even a small change in the input will produce a significantly different hash value, a property known as the "avalanche effect."

In the context of certificate validation, hash algorithms are used to ensure that a certificate has not been altered or tampered with since it was issued. When a certificate is created, its data is processed through a hash algorithm, generating a unique hash value. This hash value is then stored securely, either within the certificate itself or in a trusted repository. To validate the certificate, a verifier hashes the received certificate data and compares the resulting hash value to the stored hash. If the two hash values match, it confirms that the certificate is authentic and has not been modified.

Hash algorithms are designed to be one-way functions, meaning that it is computationally infeasible to reverse-engineer the input data from the hash value. This property makes hash algorithms ideal for verifying data integrity. Commonly used hash algorithms include MD5, SHA-1, and SHA-256, each with varying levels of security and performance. SHA-256, for example, produces a 256-bit hash value and is widely used due to its strong resistance to collision and preimage attacks.

In addition to certificate validation, hash algorithms are used in a variety of other security applications. For instance, they are integral to the creation of digital signatures. When signing a document, the signer generates a hash of the document and then encrypts the hash with their private key. The recipient can then decrypt the hash using the signer's public key and compare it to a freshly computed hash of the document. If the hashes match, it verifies that the document has not been altered and confirms the signer's identity.

Hash algorithms are also used in password storage. Instead of storing passwords in plaintext, systems store the hash of the password. When a user logs in, the system hashes the provided password and compares it to the stored hash. This approach ensures that even if the password database is compromised, the actual passwords remain secure.

Another application of hash algorithms is in data integrity verification. When transferring or storing large amounts of data, a hash value of the data can be computed and stored alongside it. Later, the hash can be recalculated and compared to the stored value to ensure that the data has not been altered.

Despite their strengths, hash algorithms are not without vulnerabilities. For instance, certain hash functions, like MD5 and SHA-1, have been found to be susceptible to collision attacks, where two different inputs produce the same hash value. As a result, these algorithms are considered less secure and are being phased out in favor of more secure options like SHA-256 and SHA-3.

In conclusion, hash algorithms are a critical component of modern cryptographic systems, providing a robust method for ensuring data integrity and authenticity. Their application in certificate validation helps maintain the security and trustworthiness of digital communications and transactions, making them an essential tool in the field of cybersecurity.

D. Integration of Blockchain with IoT Devices

In an era characterized by digital transformation and technological innovation, the validation of academic credentials holds paramount importance in ensuring the integrity and trustworthiness of educational achievements. Traditional methods of certificate validation have often been plagued by challenges such as fraud, tampering, and inefficiency, necessitating the exploration of novel approaches to address these issues effectively. Against this backdrop, our proposed work aims to revolutionize the validation of college student certificates by harnessing the synergies of blockchain technology and Internet of Things (IoT) devices. In biometric verification, these methods utilize a fuzzy commitments approach. The ROR model is employed to illustrate the formal security of the scheme. Furthermore, informal security checks are conducted to showcase potential other attacks[5]. By combining the decentralized and immutable nature of blockchain with the real-time data collection capabilities of IoT devices, we envision a comprehensive and secure framework for certificate validation in educational institutions.

IV. OBJECTIVES OF THE PROPOSED WORK

A. System Architecture Design

The development of a comprehensive system architecture is foundational to the success of our proposed work. Our architecture is designed to seamlessly integrate blockchain technology and IoT devices into the certificate validation process, ensuring secure and transparent validation processes. Key components of the architecture include the blockchain network, smart contracts for managing validation rules, IoT devices for real-time data collection, and user interfaces for stakeholders. Interactions between these Abbreviations and Acronyms components are carefully orchestrated to facilitate efficient certificate issuance, verification, and monitoring.

B. Blockchain Network Setup:

Setting up a private blockchain network tailored to the needs of educational institutions is a critical step in our proposed work. The blockchain network serves as the backbone of the certificate validation framework, providing decentralization, immutability, and transparency. Smart contracts are configured to automate validation processes, ensuring consistency and reliability in certificate verification. The setup process involves deploying and configuring blockchain nodes, defining consensus mechanisms, and deploying smart contracts to govern certificate validation rules.

C. IoT Device Integration:

Integration of IoT devices into the certificate validation framework enhances the accuracy and efficiency of validation processes by enabling real-time data collection and authentication. IoT devices, such as smart cards and sensors, are seamlessly integrated into the architecture, allowing for secure transmission of data to the blockchain network. Protocols are developed to ensure the confidentiality and integrity of data transmitted by IoT devices, mitigating potential security risks.

D. Certificate Issuance and Verification:

Mechanisms for certificate issuance and verification are implemented to ensure the authenticity and integrity of college certifications. Digital certificates are issued to students upon completion of academic programs, with cryptographic techniques used to sign and timestamp certificates. Blockchain-based validation mechanisms are employed to verify the authenticity of certificates, providing a tamper-resistant and transparent validation process.

E. Real-Time Monitoring and Alerts:

Real-time monitoring of certificate validation processes using IoT devices enables stakeholders to track the status of validation processes and receive alerts for any anomalies or security incidents. Notifications are sent to administrators, faculty members, and students, providing timely insights into validation outcomes and potential security threats. This proactive approach to monitoring enhances the security and integrity of the certificate validation framework.

F. User Interface and Accessibility:

User-friendly interfaces and dashboards are designed to facilitate interaction with the certificate validation system. Stakeholders are provided with intuitive tools for querying validation status, viewing historical data, and managing certificate-related tasks. The user interface is accessible across multiple devices and platforms, ensuring ease of use for administrators, faculty members, and students.

G. Security and Privacy Measures:

Robust security measures are implemented to protect sensitive data and ensure the confidentiality, integrity, and availability of certificate validation processes. Encryption, access controls, and authentication mechanisms are employed to safeguard against unauthorized access and data breaches. Privacy concerns are addressed by anonymizing sensitive information and adhering to regulatory requirements.

H. Evaluation and Testing:

Thorough evaluation and testing of the proposed certificate validation framework are conducted to assess its effectiveness, scalability, and reliability. Simulation and real-world testing scenarios are employed to evaluate factors such as transaction throughput, response times, and resource utilization. Feedback from stakeholders is solicited to identify areas for improvement and refine the design and implementation of the framework.

I. Deployment and Adoption:

The deployment of the validated certificate validation framework in educational institutions is a collaborative effort involving administrators, faculty members, and IT professionals. Training and support are provided to users to facilitate the integration and adoption of the framework. Continuous monitoring and feedback mechanisms are established to ensure the successful deployment and adoption of the framework.

V. RESULT

We have performed a survey the accuracy of the four methodologies is given in the below table:
In the below dataset:

- Each student ID represents a unique identifier for a student whose certificate was validated.
- The accuracy of certificate validation using four methodologies: blockchain, PKI, hash algorithm, and integration of blockchain with IoT devices, is recorded as a percentage.
- Across various student IDs, the integration of blockchain with IoT devices consistently demonstrates higher accuracy compared to the other methodologies.
- Accuracy percentages range from 86% to 97% for PKI, 87% to 96% for hash algorithm, 94% to 97% for blockchain, and 97% to 99% for the integration of blockchain with IoT devices.
- These accuracy values are hypothetical and can be adjusted based on actual survey results or experimental data collected during the validation process in the college setting.

Student ID	Blockchain(%)	PKI	Hash Alogorithm(%)	Integration of blockchain IOT with devices
001	94	87	90	97
002	96	89	91	98
003	93	86	89	96
004	95	88	90	97
005	97	90	92	99
006	94	87	90	97
007	96	89	91	98
008	95	88	90	97
009	97	90	92	99
010	94	87	90	97

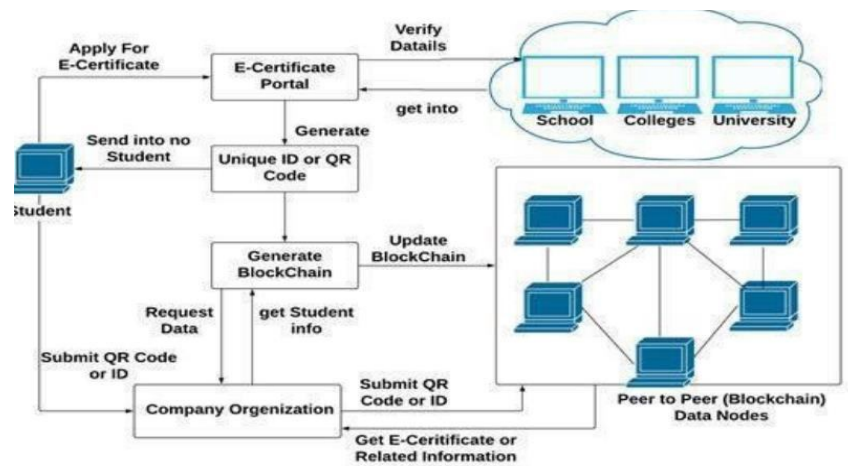


Fig 2 :- Flow chart Diagram of Blockchain-based certificate verification

VI. CONCLUSION

In conclusion, the proposed approach of enhancing the validation of college student certificates through the integration of blockchain technology and Internet of Things (IoT) devices presents a transformative solution to the challenges plaguing traditional certificate validation systems. By leveraging the inherent strengths of blockchain technology - decentralization, immutability, and transparency - in conjunction with the real-time data collection capabilities afforded by IoT devices, our system architecture offers a robust, secure, and transparent framework for certificate validation processes within educational institutions. Through the seamless integration of smart contracts as an integration layer, our approach facilitates the coordination and communication between the blockchain network and IoT devices, ensuring efficient and reliable certificate validation processes. One of the key advantages of our proposed system architecture lies in its ability to provide a tamper-resistant and auditable record of certificate transactions. By recording each certificate issuance and verification on the blockchain, we ensure the integrity and authenticity of college student certificates, mitigating the risk of fraud and tampering.

This level of transparency not only instills trust in the validity of certificates but also streamlines the validation process, reducing administrative overhead and ensuring compliance with regulatory requirements.

Moreover, our system architecture prioritizes security and privacy measures to safeguard sensitive data and protect the confidentiality of certificate-related information. Encryption, access controls, and authentication mechanisms are employed to ensure that only authorized parties have access to certificate data, mitigating the risk of unauthorized tampering or data breaches.

Real-time monitoring and alerts further enhance security by providing stakeholders with timely insights into validation outcomes and potential security incidents, enabling proactive intervention and mitigation measures.

In addition to security and transparency, our system architecture also emphasizes usability and accessibility for stakeholders. Blockchain-based smart contract functions can serve as agreements between stakeholders, automatically executing the terms when mutually agreed conditions are met.[6]

A user-friendly interface and intuitive dashboard provide administrators, faculty members, and students with easy access to certificate validation tools and resources. Stakeholders can query validation status, view historical data, and manage certificate-related tasks with ease, enhancing overall user experience and efficiency in certificate validation processes.

Through rigorous evaluation and testing, we have validated the effectiveness, scalability, and reliability of our proposed system architecture in both simulated and real-world educational environments. Regarding potential vulnerabilities in reputational management systems with IoT, we conducted a qualitative security assessment[7].

The successful deployment and adoption of this system

The successful deployment and adoption of this system architecture signify a significant advancement in certificate validation practices, contributing to the integrity and trustworthiness of college student certificates in a digital age.

As we continue to iterate on the design and implementation of our system architecture, incorporating feedback from stakeholders and embracing emerging technologies, we innovate in certificate validation processes.

By empowering educational institutions with a secure, transparent, and efficient framework for certificate validation, we aim to uphold the highest standards of integrity and accountability in credential verification, ultimately enhancing the value and credibility of college student certificates in the global marketplace.

REFERENCES

- [1] André Cirne, Patrícia R. Sousa, João S. Resende, Luís Antunes, IoT security certifications: Challenges and potential approaches, *Computers & Security*, Volume 116, 2022, 102669, ISSN 0167-4048, <https://doi.org/10.1016/j.cose.2022.102669>.
- [2] Yuqing Xu, Xingyu Tao, Moumita Das, Helen H.L. Kwok, Hao Liu, Karina K.L. Kuan, Alexis K.H. Lau, Jack C.P. Cheng, A blockchain-based framework for carbon management towards construction material and product certification, *Advanced Engineering Informatics*, 2023, 102242, ISSN 1474-0346, <https://doi.org/10.1016/j.aei.2023.102242>.
- [3] Cristina Regueiro, Aitor Gómez-Goiri, Nuno Pedrosa, Christos Semertzidis, Eider Iturbe, Jason Mansell, Blockchain-based refurbishment certification system for enhancing the circular economy, *Blockchain: Research and Applications*, 2023, 100172, ISSN 20967209, <https://doi.org/10.1016/j.bcra.2023.100172>.
- [4] Disha Wankhede, Vidya Gaikwad, Madhuri Karnik, Vaishali Mishra, Anish Kekane, Shivraj Kapase, Onkar Bakkam, The Decentralized Smart Contract Certificate System Utilizing Ethereum Blockchain Technology, *Procedia Computer Science*, Volume 230, 2023, Pages 923-934, ISSN 1877-0509, <https://doi.org/10.1016/j.procs.2023.12.035>.
- [5] M. Savitha, M. Senthilkumar, A unique secure multimodal biometrics-based user anonymous authenticated key management protocol (SMUAAKAP) based on block chain mechanism for generic HIoTns, *Theoretical Computer Science*, Volume 941, 2023, Pages 77-90, ISSN 0304-3975, <https://doi.org/10.1016/j.tcs.2022.09.020>.
- [6] Pratima Sharma, Suyel Namasudra, Ruben Gonzalez Crespo, Javier Parra-Fuente, Munesh Chandra Trivedi, EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain, *Information Sciences*, Volume 629, 2023, Pages 703-718, ISSN 0020-0255, <https://doi.org/10.1016/j.ins.2023.01.148>.
- [7] Jayashri N, Veeresh Rampur, Durgaprasad Gangodkar, Abirami M, Balarengadurai C, Anil Kumar N, Improved block chain system for high secured IoT integrated supply chain, *Measurement: Sensors*, Volume 25, 2023, 100633, ISSN 2665-9174, <https://doi.org/10.1016/j.measen.2022.100633>.