

Bogus E-Certificate Validation and Verification Using Block Chain Technology

Ms.R.Suganya, M.E
Assistant Professor, Department of CSE,
Coimbatore Institute of Technology,
Coimbatore-641014.

Janani M
Kirthika T
Nishadevi R
Selvi T
Thriyambika R
UG Students
Department of CSE, Coimbatore Institute of Technology
Coimbatore-641014

Abstract:

The "Blockchain Certificate Validation and Verification System" introduces an innovative approach to academic credential verification, leveraging blockchain technology for enhanced security, decentralization, and user control. Unlike traditional verification methods, our system stores encrypted certificate data in Firebase and Pinata, ensuring unmatched authenticity and ownership. The hash value provided by Pinata is stored on the blockchain, enabling secure and decentralized verification. Compared to existing systems, our solution offers immutability, transparency, and accountability through unalterable records for all certificate transactions. Powered by Ethereum smart contracts, it provides precise access management and customizable validation protocols. Technically, the system's frontend utilizes ReactJS, HTML, and CSS for a seamless user experience, while backend operations are managed using Node.js, Firebase and Ethereum. Certificates are uploaded and stored in Firebase and Pinata, with hash values secured on the blockchain. In addition to core functionalities, users enjoy features like certificate issuing, verification, and real-time notifications. Certificates can be designated as public or private, with an activity log for transparency. Once issued, certificates are encrypted, with metadata stored on the blockchain. Decryption keys are required for certificate validation, ensuring robust data integrity. Our system offers rapid, secure certificate validation while proving cost-effective compared to traditional methods. By harnessing blockchain technology, the "Blockchain Certificate Validation and Verification System" sets a new standard for secure, decentralized, and user-controlled credential verification with advanced technology and intuitive design.

KEYWORDS: *Transparency, Decryption keys, Ethereum smart contract, Rapid, secure certificate validation, Data integrity*

I. INTRODUCTION

In today's digital landscape, the demand for secure and efficient academic credential verification has never been greater. However, traditional verification methods often fall short in terms of data security, authenticity, and decentralization. The project we are developing, "Blockchain Certificate Validation and Verification System," aims to address these shortcomings by leveraging blockchain technology. By strategically encrypting certificate data and storing it in Firebase, Pinata, and the blockchain, this innovative system ensures unparalleled levels of data privacy and ownership. The "Blockchain Certificate Validation and Verification System" offers immutability, transparency, and accountability through unmodifiable records for all certificate transactions. Smart contracts, integrated with the Ethereum blockchain, empower the system with granular access control and specific rules for certificate validation, enhancing user control and trust. The validation process confirms whether a certificate is valid before storing it in Firebase, Pinata, and the blockchain, allowing any individual to verify the certificate as the system acts in a decentralized manner.

From a technical standpoint, the project utilizes cutting-edge frontend and backend technologies to deliver a seamless user experience and efficient certificate processing. The primary objective of the "Blockchain Certificate Validation and Verification System" project is to address data privacy and security concerns inherent in traditional credential verification methods. By emphasizing the risks associated with centralized verification providers and advocating for the importance of data security, control, and transparency, the project aims to promote the adoption of decentralized credential verification solutions. Through the integration of smart contracts and blockchain technology, the system seeks to enhance user control and foster trust in decentralized credential exchanges, offering superior scalability, validation capabilities, and cost-efficiency.

II. LITERATURE SURVEY

[1] This paper introduces NutBaaS, a Blockchain-as-a-Service platform aimed at simplifying blockchain development for developers. It offers various services such as network deployment, system monitoring, and smart contract analysis and testing. NutBaaS enables developers to focus on business logic without worrying about the complexities of maintaining and monitoring the underlying blockchain infrastructure.

[2] This paper explores the use of ontologies for modeling smart contracts, focusing on the Solidity language. It presents an ontology that defines entities in Solidity and aligns them with other standardized ontologies. By validating the ontology with deployed contracts on the Ethereum blockchain, the paper aims to enhance the interoperability and knowledge representation of smart contracts.

[3] This paper addresses the privacy and scalability challenges in blockchain-based certificate validation systems. It proposes PBCert, a privacy-preserving scheme for certificate status validation, which

separates control and storage of revoked certificates. By storing minimal control information on the blockchain and designing obscure responses to certificate status queries, PBCert aims to improve privacy while maintaining security and efficiency.

[4] This paper introduces a novel encryption scheme for medical images based on chaos and DNA encoding. The scheme involves two encryption rounds with block-based permutation, pixel-based substitution, DNA encoding, bit-level substitution, DNA decoding, and bit-level diffusion. By utilizing chaos and DNA computing, the proposed scheme aims to provide robust encryption against various attacks while maintaining low complexity for real-time applications.

III. PROPOSED METHODOLOGY

The proposed methodology for the blockchain-based certificate validation and verification system integrates advanced technologies and robust architectural principles to create a secure and efficient platform. The system is structured into distinct modules dedicated to tasks such as user authentication, certificate management, activity logging, validation, and access control, ensuring clear organization and effective functionality management.

React is employed to develop the frontend, providing an intuitive and user-friendly interface. The backend relies on Firebase for user authentication and certificate management, while blockchain technology and Pinata are used for secure data storage and integrity verification. Users authenticate on the website, upload their certificates and details, which are then validated. Valid certificates and user details are stored in Firebase, while the certificates and their hash values are generated using SHA and IPFS algorithms with Pinata. The hash values are recorded on the blockchain to ensure data integrity and security.

For verification, any organization, institution, or individual can upload a certificate to obtain its hash value. This hash value is compared with the blockchain-stored hash value in the verification module, and a match verifies the certificate. The integration of blockchain technology enhances transparency and traceability, reinforcing the system's commitment to security and accountability, thereby bolstering user trust in the decentralized certificate validation platform.

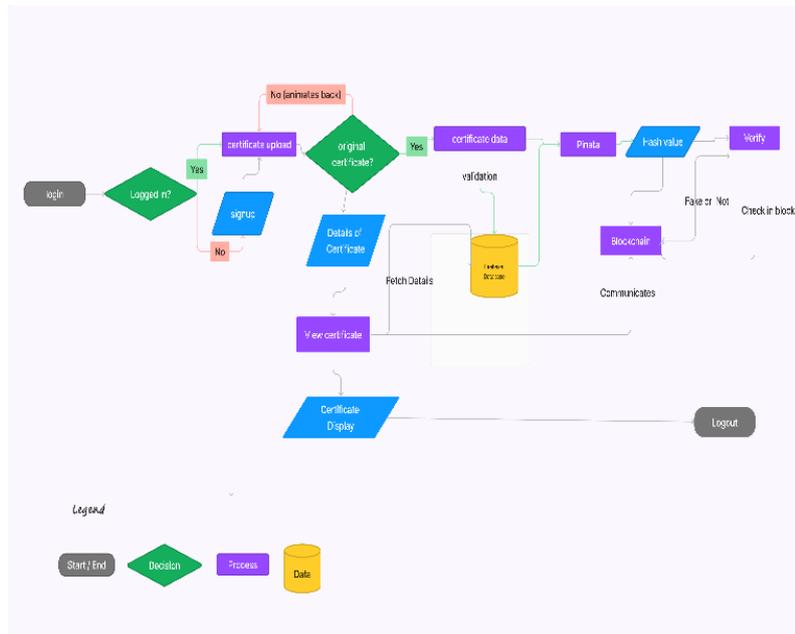


Fig.1 System Architecture

IV. IMPLEMENTATION

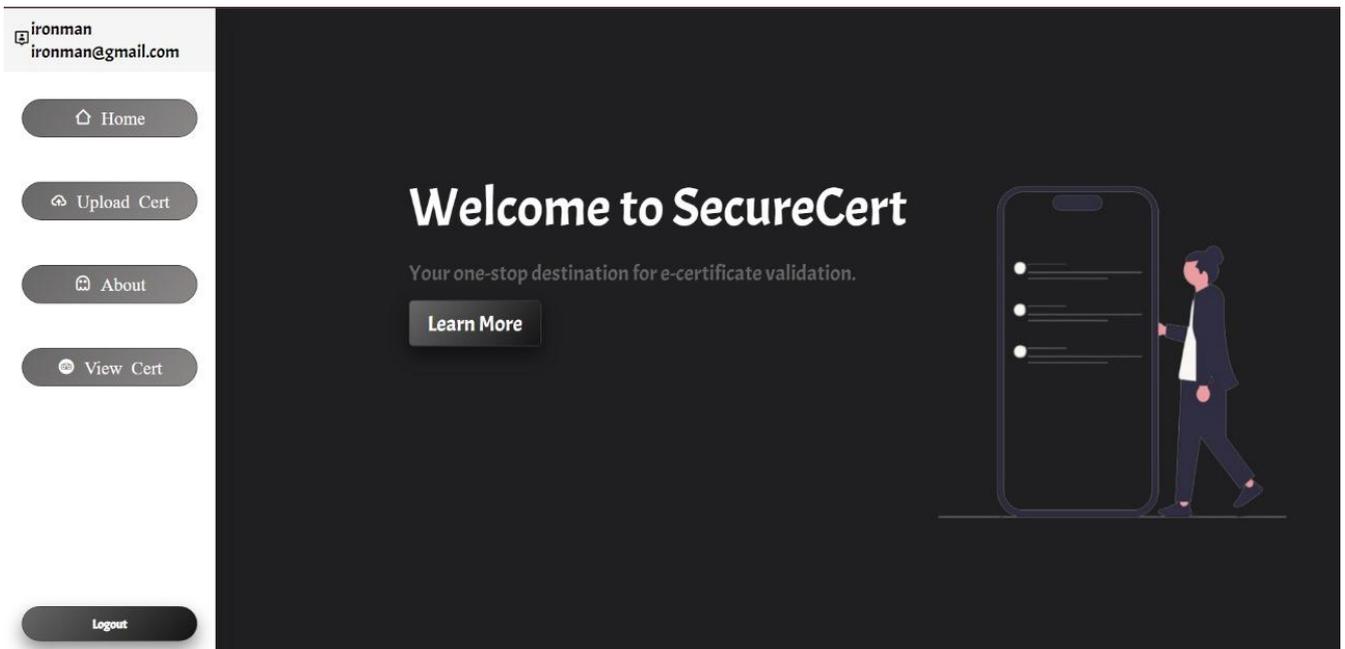


Fig 2. Home page

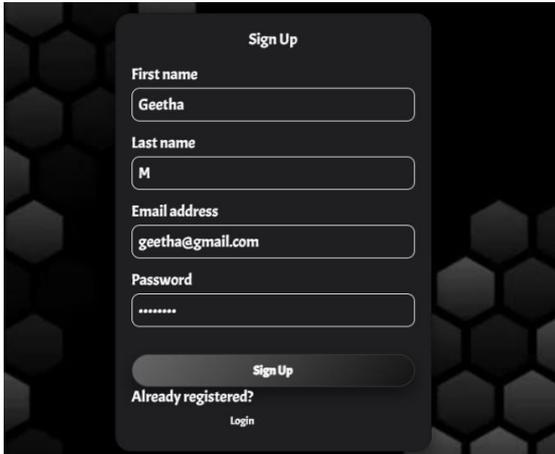


Fig 3. SignUp Page

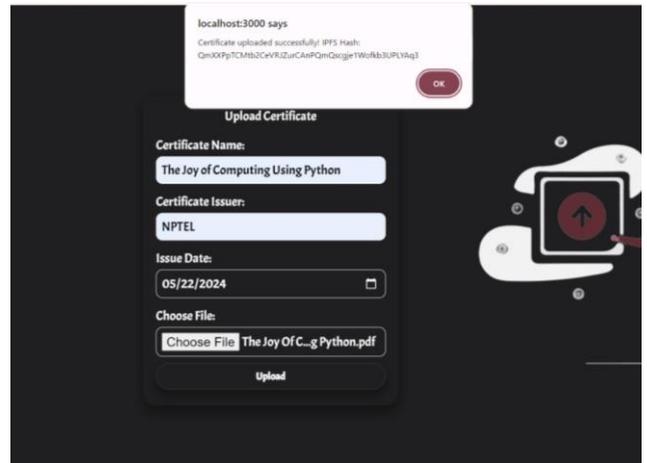


Fig 5. Upload Certificate Page

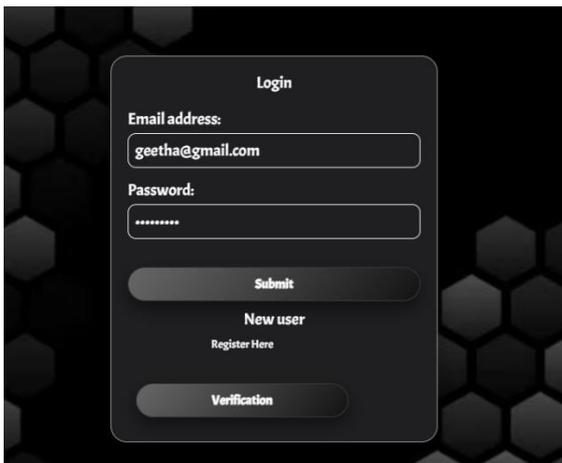


Fig 4. Login Page

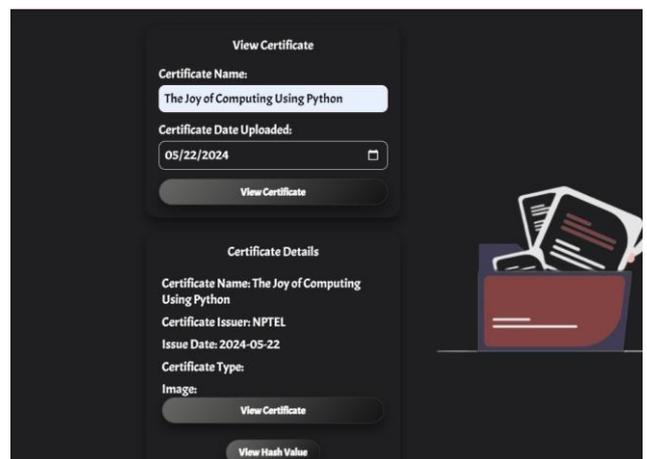


Fig 6. View Certificate Page

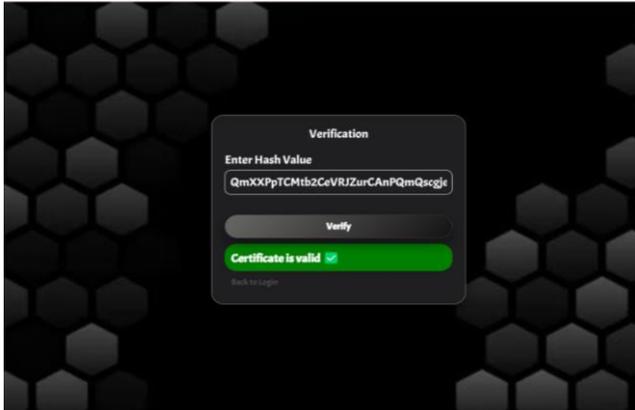


Fig 6.Verification page(valid)

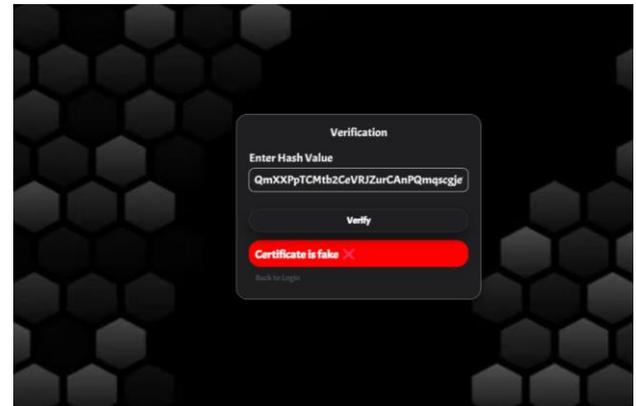


Fig 7.Verification page(Fake)

V. CONCLUSION

The project endeavours to establish a robust and decentralized certificate validation and verification system, leveraging advanced technologies like blockchain, Pinata, and Firebase. While addressing challenges such as user adoption and scalability, the system prioritizes efficiency in certificate validation processes. Looking forward, future innovations will focus on optimizing performance and overcoming existing limitations to ensure the system's continual evolution and relevance in the dynamic realm of decentralized technology. This commitment underscores our dedication to enhancing security, transparency, and user trust in credential verification processes, paving the way for broader adoption of decentralized solutions in the digital age.

VI. FUTURE WORK

1. Smart Contract Upgrades:

- Manage certificate expiration and renewal.
- Add multi-factor authentication for better security.

2. Multi-Blockchain Support:

- Connect with Binance Smart Chain.
- Connect with Polkadot.

3. Scalability Improvements:

- Use sharding to handle more users.
- Optimize performance for larger data loads.

VII. REFERENCES

- [1] NutBaaS: A Blockchain-as-a-Service Platform: WEILIN ZHENG, ZIBIN ZHENG, XIANGPING CHEN, KEMIAN DAI, PEISHAN LI, AND RENFEI CHEN
- [2] Toward the Ontological Modeling of Smart Contracts: A Solidity Use Case: JUAN CANO-BENITO, ANDREA CIMMINO, AND RAÚL GARCÍA-CASTRO
- [3] PBCert: Privacy-Preserving Blockchain-Based Certificate Status Validation Toward Mass Storage Management: SHIXIONG YAO, JING CHEN, KUN HE, RUIYING DU, TIANQING ZHU, AND XIN CHEN
- [4] Novel Medical Image Encryption Scheme Based on Chaos and DNA Encoding: AKRAM BELAZI, MUHAMMAD TALHA, SOFIANE KHARBECH, AND WEI XIANG
- [5] Survey on Blockchain Based Digital Certificate System NEETHU GOPAL, VANI V PRAKASH (IRJET)
- [6] Zibin Zheng Shuang Ning Dai, Xiangping Chen, "An Overview of Blockchain Technology: hite 2017. Consensus, and Future Trends". IF International Congress on Data.
- [7] Jiin-Chiou, Narn-Yih Lee, Chien Chi, YI-Hua Chen, "Blockchain and Smart Contract for Digital Certificate," Proceedings of IEEE International Conference on Applied System Innovation 2018.
- [8] Maharshi Shah, Priyanka Kumar, "Tamper Proof Birth Certificate Using Blockchain Technology", International Journal of Recent Technology and Engineering (IURTE), Volume- 7. Issue-5S3, February 2019.
- [9] Stuart Haber, W. Scott Stornetta, "How to timestamp a Digital Document", Advances in Cryptology Heidelberg 1991 CRYPTO '90, LNCS 537, pp. 437-455, 1991. © Springer-Verlag Berlin