Current Journal of Engineering and Science Research
Volume 3, Issue 3, pp 15-21, March 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.303003
Available Online at https://www.cjesr.com

Blockchain Based Certificate Generation and Validation System For Refugees

[1]Y. Mohan Das, [2]U. Laxmi Chaitanya, [3]N. Naga Sai Shalini, [4]R. Pavithra, [5]G. Venu, [6]K. kishore

[1,2,3,4,5,6]Department of Computer Science Engineering (Cyber Security), GATES Institute of Technology, Gooty, Andhra Pradesh, India
E-mails: [1]mohandassonu@gmail.com, [2]Chaitanyauppala6@gmail.com, [3]shalininalamaru2005@gmail.com, [4]pavitrapavi95563@gmail.com, [5]venu148878@gmail.com, [6]kammarakishore2002@gmail.com

Abstract: The global refugee crisis has created unprecedented displacement, making access to essential services like education, healthcare, and employment challenging due to unreliable identification. Traditional certification methods are prone to forgery, loss, and accessibility issues. This project introduces a Blockchain-based Certificate Generation and Validation System for refugees, utilizing MetaMask for digital identities, the Solidity compiler on Remix IDE for certificate generation, and Ganache and Truffle for development and testing. The Django- developed frontend enables user-friendly certificate generation and validation. This system enhances security, integrity, and efficiency, reducing human errors and streamlining administrative procedures. By providing secure, verifiable certificates, it improves refugees' access to essential services and supports their integration into new communities, offering a scalable solution to certificate management in refugee contexts.

Keywords: Blockchain, Certificate Generation, Certificate Validation, Refugees, Digital Identity, Smart Contracts.

I. INTRODUCTION

The global refugee crisis has led to unprecedented displacement, with millions fleeing conflict, persecution, or natural disasters, facing significant challenges in accessing essential services due to unreliable identification. Traditional methods of issuing certificates are prone to forgery, loss, and accessibility issues. This project introduces a Blockchain-Based Certificate Generation and Validation System for refugees, leveraging blockchain's decentralised and immutable characteristics to provide secure, tamper-proof, and easily verifiable certificates. The system stores certificates on the Ethereum blockchain, utilizing smart contracts written in Solidity and compiled with the Remix IDE to automate issuance and validation, enhancing security and integrity while streamlining administrative processes and reducing human error. A user-friendly interface developed with Django enables seamless interaction for refugees and authorized entities. This project demonstrates modern technology's potential to address critical humanitarian issues by providing refugees with reliable and verifiable certificates, significantly improving their access to essential services and supporting their integration into new communities. Blockchain technology's key features, including decentralization, immutability, transparency, and security, make it ideal for applications requiring trust and integrity. Refugees often struggle to prove their identity, education, and work credentials due to unreliable traditional paper- based certificates. Blockchain offers a secure, transparent way to generate, store, and validate certificates, ensuring quick and reliable verification and improving access to opportunities and services.

The project's primary objectives are to provide a secure, tamper-proof method for generating and storing certificates, enable easy and reliable verification by relevant authorities, and utilise decentralised blockchain technology for integrity and transparency. The system utilizes MetaMask for secure interactions with the Ethereum blockchain, Solidity for writing smart contracts, Remix IDE for developing and managing smart contracts, Ganache for controlled testing, and Truffle for compiling, deploying, and testing smart contracts. By providing refugees with reliable and verifiable certificates, this system aims to improve their access to essential services and support their integration into new communities, contributing to their overall well-being and stability.

II. RELATED WORK

The proposed system builds on a growing body of research that applies blockchain technology to digital certificates, identity management, and refugee support. Mohamed et al. present a

Current Journal of Engineering and Science Research
Volume 3, Issue 3, pp 15-21, March 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.303003
Available Online at https://www.cjesr.com

certificate generator using blockchain (BlockCert) to digitize student data and automate verification, significantly reducing waiting times and mitigating certificate forgery in the Egyptian education system. Their work demonstrates that anchoring credentials on a public blockchain can improve trust and efficiency in academic environments, but it is not tailored to the specific constraints and vulnerabilities of displaced populations.

Several authors have explored blockchain-based certificate validation platforms that use Ethereum, smart contracts, and QR codes to enable decentralized verification of academic credentials. Swetha and Priya propose an online certificate validation system that employs Ethereum and smart contracts to guarantee integrity and prevent tampering, showing that blockchain can replace manual verification workflows with automated, transparent checks. Cheng et al. investigate blockchain and smart contracts for academic certificates more broadly, highlighting benefits such as security and transparency but also stressing challenges around privacy, immutability, and regulatory compliance that must be addressed before large-scale adoption. Beyond pure education contexts, work on digital identities in asylum and migration procedures has shown that blockchain can streamline verification and reduce administrative overhead. Amend et al. study digital and blockchain-based certification processes in the asylum procedure, reporting easier verification of document validity, stronger protection against forgery, protection against forgery, and reduced manual effort, while emphasizing that legal and procedural constraints and procedural constraints must still be respected. Omoka demonstrates how permissioned blockchain (Hyperledger Fabric) can consolidate and share population data across Kenyan agencies, solving duplication and consistency issues that arise with traditional relational databases and illustrating blockchain's value as an immutable, shared ledger for sensitive records.

A parallel line of research focuses on self-sovereign identity (SSI) and digital identity for migrants and refugees. Corte-Real et al. review blockchain applications in migrant and refugee health, concluding that blockchain can improve identity management and health record availability, but also pointing to open challenges in usability, interoperability, and data protection. Syed discusses how blockchain-based digital identity can empower disadvantaged individuals by giving them decentralized control over their credentials, while Forti examines regulatory and fundamental rights issues in blockchain-driven identification systems in migration contexts. Sæbø further argues that humanitarian digital identities based on blockchain can improve efficiency and transparency in managing refugee identities, though scalability and governance remain open questions.

Compared to these works, the present project specifically targets certificate generation and validation for refugees by combining Ethereum smart contracts, MetaMask-based digital wallets, and a Django web front end into one integrated system. It adapts ideas from academic blockchain certificate systems to a humanitarian setting, where refugees may lack stable documentation, and aligns with SSI and digital identity literature by allowing recipients to hold verifiable certificates in their own wallets rather than relying solely on centralized databases. In doing so, it fills a gap between general academic credential solutions and broader identity frameworks, focusing on a concrete, deployable mechanism for securely issuing and validating refugee certificates across borders.

III. PROPOSED SYSTEM

The proposed system introduces a blockchain-based platform for generating and validating digital certificates to ensure security, transparency, and authenticity. In this system, authorized institutions such as government agencies, NGOs, or educational organizations act as certificate issuers and generate digital certificates for individuals, particularly refugees who may lack reliable documentation. When a certificate is issued, its details are converted into a cryptographic hash and stored on the blockchain using smart contracts. Because blockchain data is immutable, the stored certificate information cannot be altered or forged, ensuring the integrity of the records. The system uses technologies such as Ethereum blockchain, Solidity smart contracts, MetaMask for wallet integration, and tools like Remix, Ganache, and Truffle for development and testing. A web-based interface built using Django, HTML, and CSS allows issuers to upload certificates and enables users or organizations to verify them easily. During verification, the system compares the certificate's hash with the hash stored on the blockchain to confirm its authenticity. This approach eliminates the need for centralized verification systems, reduces the risk of fraud, and provides a secure and reliable method for managing and validating certificates.

IV. SYSTEM ARCHITECTURE

The system architecture of the proposed blockchain- based certificate generation and validation system is designed to

Current Journal of Engineering and Science Research
Volume 3, Issue 3, pp 15-21, March 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.303003
Available Online at https://www.cjesr.com

provide a secure, transparent, and decentralized platform for issuing and verifying digital certificates. The architecture consists of several key components including the certificate issuer, certificate holder, verifier, web application interface, blockchain network, and smart contracts. The certificate issuer, such as a government agency, educational institution, or NGO, is responsible for generating and issuing digital certificates to users. The system uses a web-based application developed with technologies such as Django for the backend and HTML and CSS for the frontend, which allows authorized issuers to upload certificate details into the system. Once a certificate is created, its data is converted into a cryptographic hash and stored on the blockchain using smart contracts written in Solidity. The blockchain network, typically implemented using Ethereum, ensures that the certificate information is immutable and cannot be altered or tampered with. Users or certificate holders receive their digital certificates and can share them with organizations when verification is required. The verification process involves checking the certificate hash stored on the blockchain to confirm its authenticity and integrity. Wallet integration using MetaMask is used to manage blockchain transactions and user identities. Development and testing of the system are carried out using tools such as Remix IDE, Ganache, and Truffle, while a lightweight database such as SQLite is used to manage application-level data. This architecture ensures a secure and efficient method for certificate issuance and validation while eliminating the risks associated with traditional paper-based systems.

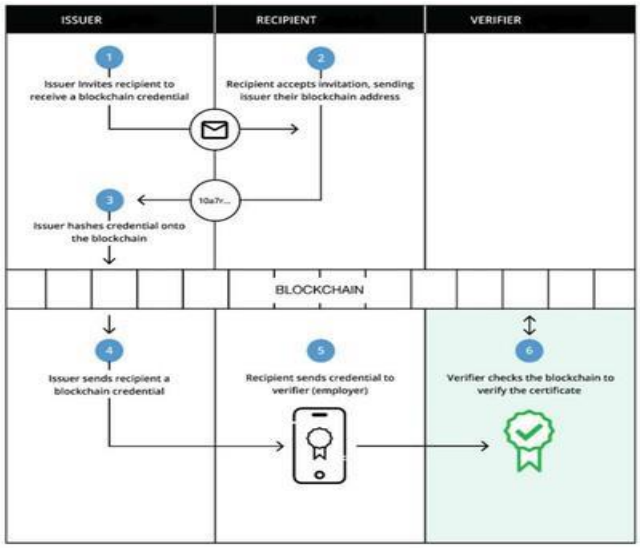

Figure 1: Architecture Design of the proposed system

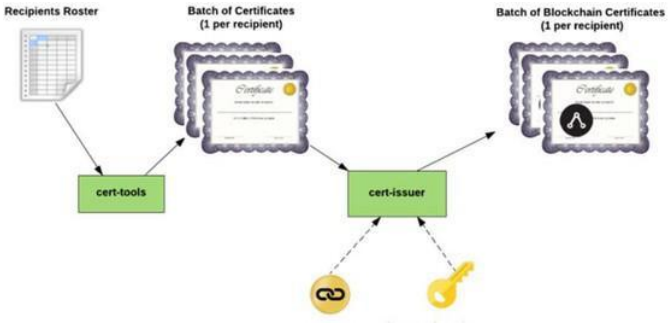

Figure 2: Use Case Diagram of the proposed system

V. IMPLEMENTATION

The implementation of the proposed work focuses on developing a blockchain-based certificate generation and validation system that ensures secure and tamper- proof certificate management. The system is implemented using a combination of web technologies, blockchain platforms, and smart contracts. Initially, a web application is developed using Django for the backend and HTML and CSS for the frontend to provide a user-friendly interface for certificate issuance and verification. Authorized institutions such as educational organizations, government bodies, or NGOs act as certificate issuers and log into the system to generate digital certificates for users. When a certificate is created, the certificate details are processed and converted into a cryptographic hash to ensure data integrity. This hash is then stored on the blockchain using smart contracts written in Solidity. The blockchain platform used for the implementation is Ethereum, which provides decentralization and immutability, ensuring that once the certificate information is stored it cannot be modified or tampered with. To interact with the blockchain network, MetaMask is used as a digital wallet that manages user authentication and transaction signing. For development and testing purposes, tools such as Remix IDE, Ganache, and Truffle are used to write, deploy, and test smart contracts in a local blockchain environment. The system also uses a lightweight database such as SQLite to manage application-level data such as user details and certificate records. During the verification process, the verifier uploads or enters the certificate details into the system, and the system compares the generated hash with the hash stored on the blockchain. If the hashes match, the certificate is considered valid and authentic. Through this implementation, the system provides a reliable and secure method for issuing and validating digital certificates while reducing the risk of fraud and document forgery.

Current Journal of Engineering and Science Research
Volume 3, Issue 3, pp 15-21, March 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.303003
Available Online at https://www.cjesr.com

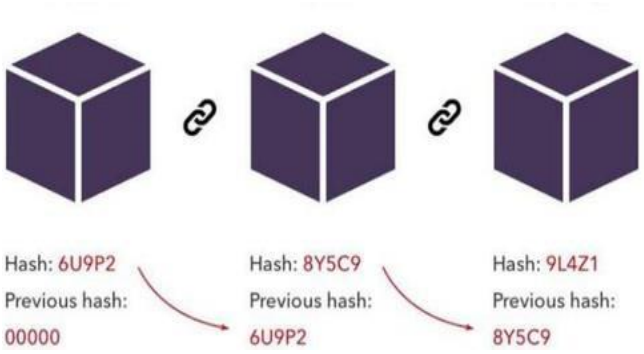

Figure 3: Blockchain Representation

VI. RESULTS

The results of the implemented blockchain-based certificate generation and validation system demonstrate that the platform successfully provides a secure and reliable method for issuing and verifying digital certificates. The system allows authorized institutions to generate digital certificates through a web-based interface and securely store the certificate hash on the blockchain. This approach ensures that the certificate information cannot be altered once it is recorded, thereby maintaining the integrity and authenticity of the data.

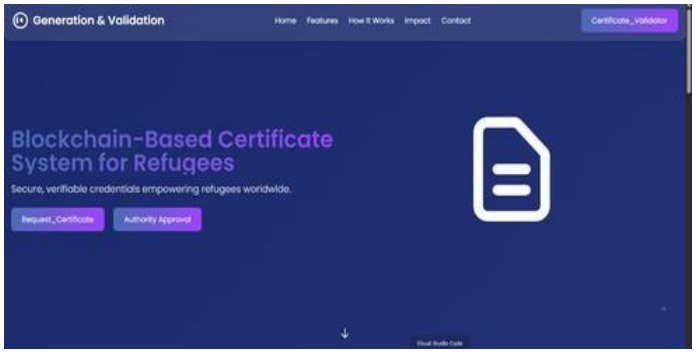

Figure 4: Project Interface

During the testing phase, the system was deployed in a local blockchain environment using development tools such as Ganache, Remix IDE, and Truffle. The web application built using Django successfully interacted with the blockchain network through smart contracts written in Solidity. The integration of the frontend and backend components enabled issuers to upload certificate details and store the corresponding hash on the blockchain without difficulty.

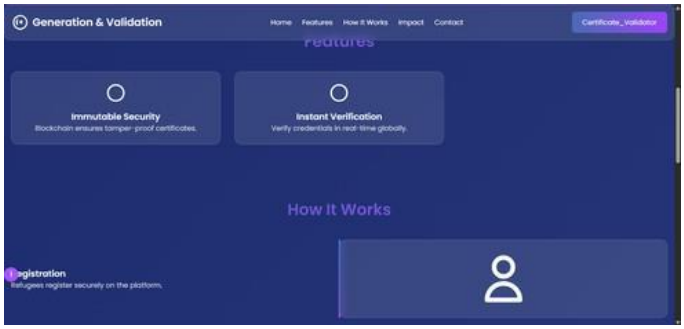

Figure 5: About the project

Figure 6: Admin credentials

The verification process also produced effective results. When a verifier entered or uploaded certificate information into the system, the application generated a hash of the provided certificate and compared it with the hash stored on the blockchain. If both hashes matched, the system confirmed that the certificate was authentic and had not been modified. This process demonstrated the ability of the blockchain system to prevent certificate forgery and provide instant verification.

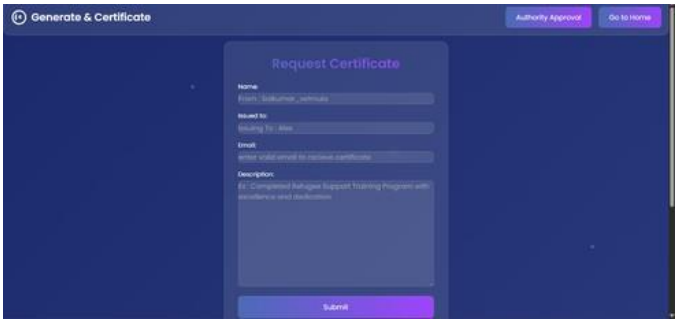

Figure 7: Refugee details

The use of MetaMask for wallet integration allowed secure interaction with the blockchain network and ensured that only

Current Journal of Engineering and Science Research
Volume 3, Issue 3, pp 15-21, March 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.303003
Available Online at https://www.cjesr.com

authorized users could perform certificate-related transactions. The system also maintained application-level data such as user information and certificate metadata using a lightweight database. This combination of blockchain storage and traditional database management improved system efficiency and usability.

Figure 8: Accepting certificate

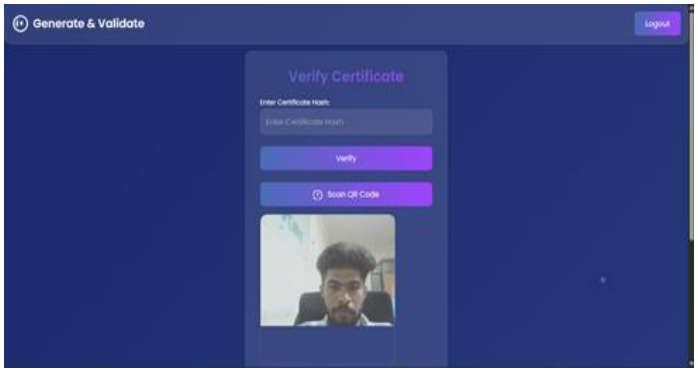

Figure 9: ID verification

Figure 10: Approved the certification

The implementation of the system was marked by the successful integration of various technologies, including front-end tools like HTML and CSS, the Django framework, and blockchain components such as Ganache and MetaMask. The application achieved its primary goal of providing a secure and transparent method for generating and verifying certificates for refugees. The clean and intuitive design of the user interface, as illustrated in the homepage and guide sections, contributed to a seamless user experience, enabling users to navigate the system effortlessly. The guide and FAQs sections played a crucial role in educating users about the application and the underlying blockchain technology, ensuring they could utilize the system effectively

The back-end functionalities, demonstrated through the Django admin interface and the blockchain tools, were robust and reliable. Ganache allowed for thorough testing of smart contracts and transactions, ensuring that the blockchain interactions were accurate and secure before deployment. The snapshots of Ganache transactions and the certificate generation process showed that the system correctly recorded and managed transactions, enhancing transparency and trust. The generated certificates, both in their design and data accuracy, met the project's objectives of providing a professional and readable document for refugees.

Verification of certificates was efficiently handled by the system, with results being accurately displayed to users. This process not only confirmed the authenticity of the certificates but also reinforced the system's integrity by providing a reliable means of validating the issued documents. The Django admin interface further facilitated effective management of user data and interactions, integrating seamlessly with the blockchain data to ensure smooth operational flow.

Overall, the project demonstrated a successful implementation of a blockchain-based system for certificate management, combining effective front-end design, robust back-end functionality, and secure blockchain interactions. The system’s design and technology choices ensured a user friendly experience, while the backend and blockchain components provided reliable and transparent certificate issuance and verification. Future work could focus on enhancing scalability and exploring additional features to further refine and expand the system’s capabilities.

Current Journal of Engineering and Science Research
Volume 3, Issue 3, pp 15-21, March 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.303003
Available Online at https://www.cjesr.com

Figure 11: Refugee certificate

VII. CONCLUSION

The project marks a notable advancement in addressing the challenges refugees face when validating their educational and professional credentials. By harnessing blockchain technology, the system offers a secure, decentralized, and immutable solution for issuing and validating certificates, significantly reducing the risks associated with document fraud and loss. This innovative approach ensures that refugees can reliably present their qualifications to potential employers, educational institutions, and other entities, which facilitates their integration into new communities and job markets. The project demonstrates the potential of blockchain technology to serve as a powerful tool for social good, providing marginalized populations with the means to rebuild their lives with greater dignity and confidence. This success underscores blockchain's role in fostering more inclusive and equitable systems on a global scale.

REFERENCES

[1] M. S. Mohamed, M. S. Abdiwahab, and R. Elgohary, "Certificate Generator using Blockchain Technology (BlockCert)," Special Issue Published in Int. Jnl. Of Advanced Networking & Applications (IJANA), pp. 132-135. https://journals.ekb.eg/article_342006.html

[2] S. Pu and J. S. L. Lam, "The benefits of blockchain for digital certificates: A multiple case study analysis," Technology in Society, vol. 72, p. 102176, 2023. https://www.sciencedirect.com/science/article/pii/S0160791X 22003177

[3] N. Swetha and S. Priya, "Online Certificate Validation Using Blockchain," Special Issue Published in Int. Jnl. Of Advanced Networking & Applications (IJANA), pp. 132-135. https://old.ijana.in/sp-2.php

[4] J.-C. Cheng, N.-Y. Lee, C. Chi, and Y.-H. Chen, "Blockchain and smart contract for digital certificate," in 2018 IEEE International Conference on Applied System Invention (ICASI), pp. 1046-1051, 2018. https://www.researchgate.net/publication/326705202_Blockch ain_and_smart_contract_for_digital_certificate

[5] J. Amend, M. Federbusch, G. Fridgen, F. Köhler, A. Rieger, V. Schlatt, and C. van Dun, "Digitization of certification processes in the asylum procedure by means of digital identities: A feasibility study by Germany's Federal Office for Migration and Refugees," German Federal Office for Migration and Refugees, 2021. https://www.researchgate.net/publication/389859295_Blockchain-Based_Certificate_Generation_and_Validation_System_for_Refugees

[6] A.Corte-Real, T. Nunes, and P. R. da Cunha, "Blockchain technology in migrant and refugee health: A scoping review," Journal of Global Health, vol. 12, 2022. https://www.sciencedirect.com/science/article/pii/S2666776224003594

[7] Syed, H. (2019). Power to The People: How Blockchain Based Digital Identity Can Empower Disadvantaged Individuals. https://scholar.google.co.in/scholar?q=Syed,+H.+(2019).+Power+to+The+People:+How+Blockchain+Based+Digital+Identity+Can+Empower+Disadvantaged+Individuals.&hl=en&as_sdt=0&as_vis=1&oi=scholart

[8] R. S. A. Omoka, "Application of permissioned blockchain technology on population data consolidation and sharing," Doctoral dissertation, Strathmore University, 2020). https://su-plus.strathmore.edu/items/2d42c974-7bd0-475b-b7ef-bed026291f4a

[9] Ø. Sæbø, "From promise to practice: humanitarian digital identities in the forced migration context," Master's thesis, University of Agder, 2023. https://www.scribd.com/document/600489465/2022-Book-ScientificFoundationsOfDigital

Current Journal of Engineering and Science Research
Volume 3, Issue 3, pp 15-21, March 2026
ISSN (online): 3049-1738
DOI: https://doi.org/10.47001/CJESR/2026.303003
Available Online at https://www.cjesr.com

Citation of this Article:

Y. Mohan Das, U. Laxmi Chaitanya, N. Naga Sai Shalini, R. Pavithra, G. Venu, & K. kishore. (2026). Blockchain Based Certificate Generation and Validation System For Refugees. *Current Journal of Engineering and Science Research*. 3(3), 15-21. Article DOI: https://doi.org/10.47001/CJESR/2026.303003

***** End of the Article *****