Certificate Authentication System using Blockchain Technology

Md.Amreen Ahmed,Namra Fathima
CSE
KL University
Vijayawada, India
Email: amreenahmedcse@gmail.com

***Abstract*—In the era of digital education and recruitment, forged educational and professional certificates are becoming increasingly prevalent. This project presents a blockchain-based certificate verification solution where universities, colleges, and office authorities can upload original certificate data to a decentralized ledger. Users or verifiers can enter certificate IDs or candidate names via a government-affiliated website to confirm their authenticity. The use of Ethereum blockchain, MetaMask, and smart contracts ensures transparency, tamper-resistance, and secure public accessibility. This solution benefits students, institutions, and employers by eliminating document forgery and simplifying validation processes.**

Index Terms—Blockchain, MetaMask, Ganache, Solidity, Certificate Verification, Smart Contracts

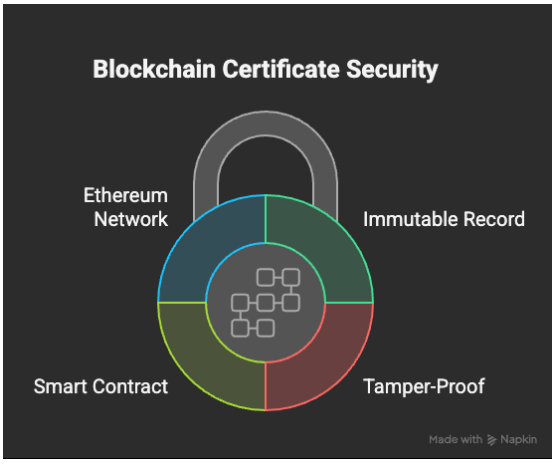
***Index Terms*—Blockchain, Metamask, Ganache, Decentralization, Smart Contracts.**

I. Introduction

The rise in forged degrees, mark sheets, and fake experience letters has created trust issues in academic and recruitment domains. Employers, universities, and government bodies often face difficulty validating a person's credentials due to inefficient, centralized, and paper-based systems.

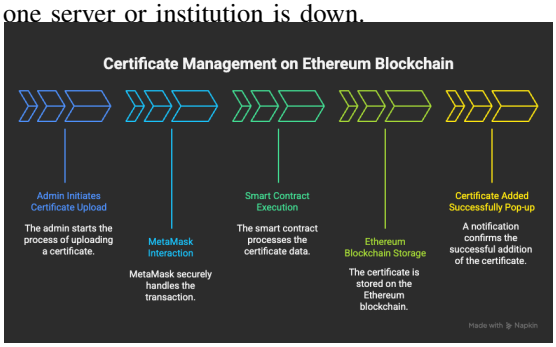
Blockchain provides a revolutionary solution by offering a decentralized, immutable ledger system. This technology ensures that once a certificate is added to the blockchain, it can never be modified or removed, thereby maintaining its authenticity. With the proposed system, a university or office can upload certificate data, and any stakeholder can verify it by entering a certificate ID or candidate name on a government-affiliated portal.

This transparent and tamper-proof mechanism helps institutions establish trust, reduce document fraud, and streamline the verification process for all stakeholders. Additionally, it promotes long-term record preservation by storing certificates in an immutable format. Organizations can avoid the time-consuming manual verifications, especially during admissions or recruitment seasons. The use of a blockchain ledger also enhances traceability, allowing audits and compliance checks to be more efficient and reliable. Moreover, the system can act as a single source of truth for government bodies during identity verification processes such as passport issuance or public sector recruitment. By maintaining a decentralized and unified certificate database, it eliminates the dependency on physical document verification and lowers the chances of administrative errors. As a result, the system contributes to a more transparent, accountable, and digitally empowered verification ecosystem.



Blockchain is a decentralized digital ledger that records transactions in a secure, transparent, and tamper-proof manner. In the context of certificate verification, when a university

or company issues a certificate, the data—such as the student's name, course, marks, issuing institution, and date—is converted into a unique digital fingerprint (hash) and stored in a block on the blockchain. This block is then linked to the previous block using cryptographic algorithms, forming a secure chain of data. Each block contains a timestamp and a reference to the previous block, making it virtually impossible to alter past records without changing every block that follows. The use of smart contracts further enhances automation and security, as these are self-executing codes deployed on the blockchain that ensure only authorized institutions can add data. Once uploaded, the certificate becomes immutable—meaning it cannot be edited or deleted. When a student or employer wants to verify a certificate, they simply enter the certificate ID or student name on a public portal. The system fetches the data directly from the blockchain and checks its validity. If the certificate exists and was uploaded by an authorized entity, the system confirms it as genuine. Otherwise, it flags the record as fake or non-existent. This removes the need for manual verification, eliminates dependence on third-party validators, and ensures trust in a decentralized, transparent environment. Blockchain's distributed nature also means the data is available globally, 24/7, and is not lost even if one server or institution is down.



II. Literature Survey

The traditional approach to certificate verification relies heavily on centralized databases, physical document inspections, and manual processes, all of which are time-consuming, prone to human error, and vulnerable to forgery. With the increase in digital applications for education and employment, the limitations of conventional systems have become more evident.

According to Kshetri (2018), blockchain technology offers significant advantages in ensuring data integrity, security, and transparency across supply chains. These same principles can be applied to the education and employment sectors, particularly for the verification of academic and professional credentials. He emphasizes that decentralization and immutability are core strengths that help prevent data tampering.

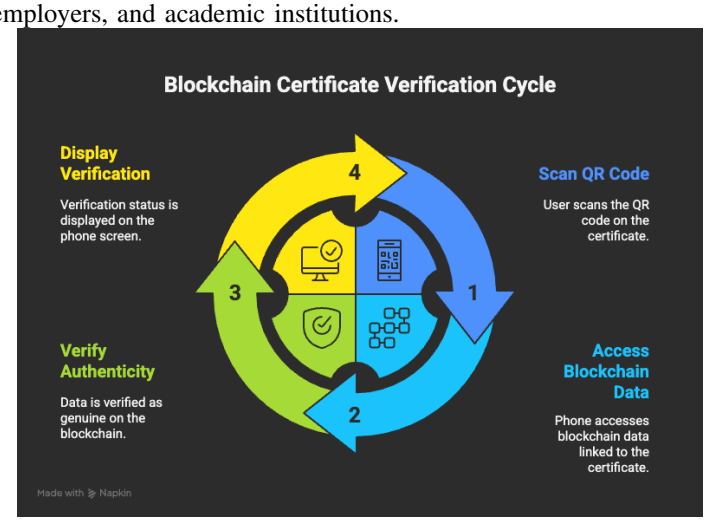
Tseng et al. (2020) proposed a blockchain framework for food traceability, which demonstrated how blockchain could offer consumers accurate product histories. Though applied in a different domain, the concept of using a distributed ledger for traceable, tamper-proof data has a strong parallel in certificate authentication systems.

Projects like MIT Media Lab's Digital Diploma and the Blockcerts open standard have already explored blockchain-backed academic certificates. These initiatives proved the feasibility of issuing and verifying certificates on public blockchain networks. However, they often require significant technical knowledge and are not integrated with government portals or widely adopted across institutions.

IBM's Blockchain Credentialing and the VeChain Foundation's work in supply chain transparency further validate blockchain's reliability in securely recording verifiable data. Yet, many of these platforms operate in private or consortium blockchains, limiting their accessibility to the public.

Despite these advancements, most existing systems lack user-centric features such as real-time verification portals, integration with web3 wallets like MetaMask, or the flexibility to search by both certificate ID and candidate name. Furthermore, they often do not support cross-sector scalability across universities, companies, and government bodies.

Hence, our proposed system addresses these gaps by using the Ethereum blockchain, MetaMask for authentication, and a web-based frontend to provide a seamless, decentralized, and transparent certificate verification experience to the public, employers, and academic institutions.



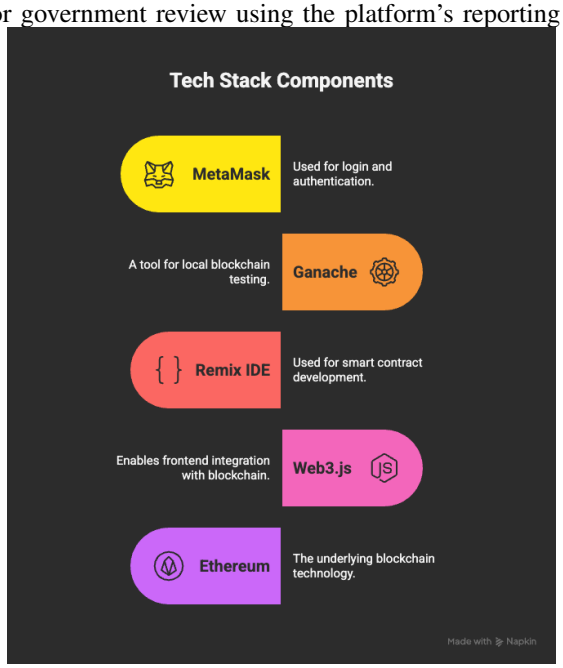
III. Methodology

In order to safeguard consumers in the areas of electronics, auto parts, and food items, this research focuses on developing a blockchain-based fake product identification system. The main objective is to provide a transparent, safe, and government-affiliated platform that allows users to use a product's product ID or name to confirm its legitimacy. The process uses the immutability, decentralization, and trustless verification that are intrinsic to blockchain technology to create a system that is both publicly accessible and impenetrable.

The manufacturer or authority uploads comprehensive product data to the blockchain after verification. The product name, product ID, brand name, manufacturing and expiration dates, and, in the case of food products, the chemical formula are all included in this data. Smart contracts, which are self-executing programs installed on the blockchain, are used to

hash and safely store all of this data. In order to preserve system integrity, these smart contracts also enforce regulations like prohibiting duplicate entries, managing data access, and verifying manufacturer credentials.

Through a web application, users can access the platform and enter the name or ID of a product to verify its legitimacy. The system retrieves the relevant information from the blockchain and uses the digital signature of the manufacturer to confirm it. The system alerts the user that the product may be phony if the record is authentic; if not, it shows a verified message. Users can flag suspected counterfeit goods for government review using the platform's reporting feature.



System Overview The proposed certificate verification system is built on top of the Ethereum blockchain using smart contracts, ensuring secure and tamper-proof recordkeeping. The entire system comprises multiple integrated components that work together to issue, store, and verify certificates in a decentralized environment.

Certificate Issuance (Admin Panel): Verified authorities such as universities or offices act as administrators. These admins access the system through MetaMask, a browser-based cryptocurrency wallet that authenticates their identity and allows them to interact with the blockchain securely. Once logged in, the admin can upload certificate details, including the candidate's name, course, institution, certificate ID, and issue date. This data is then submitted to a Solidity smart contract, which stores it immutably on the Ethereum blockchain.

Smart Contract Functionality: A custom smart contract written in Solidity is deployed on the blockchain to manage certificate records. It defines rules for adding new certificates, checking for duplicate entries, and verifying existing records. Only authorized admins can call functions like addCertificate(). The smart contract also includes a verification function verifyCertificate() that returns whether a certificate ID is valid or not.

Blockchain Storage: Each certificate is stored on the Ethereum blockchain as part of a decentralized, immutable ledger. Once a certificate is recorded, it cannot be edited or deleted. This ensures high security, prevents forgery, and allows lifelong record availability regardless of institutional changes.

User Verification Interface (Frontend): A web-based user interface is provided for students, employers, and third-party verifiers. Users can enter a certificate ID or student name to retrieve the certificate's authenticity status. The frontend communicates with the blockchain using Web3.js, allowing real-time verification directly from the blockchain network.

Testing Environment - Ganache: During development, Ganache is used as a local Ethereum network to simulate blockchain transactions without incurring real gas costs. This allows for safe and cost-effective testing of smart contracts and the entire system flow before deploying it to the mainnet or a public testnet like Sepolia or Goerli.

Security and Privacy: The system ensures that only authorized institutions can issue certificates. Unauthorized attempts to upload or alter data are automatically rejected by the smart contract. Additionally, no sensitive student data (like grades or ID proof) is made public — only essential certificate attributes are stored for validation purposes.

Transparency and Traceability: Every transaction made through the admin interface is recorded on the blockchain, providing a transparent log of certificate issuances. Since the ledger is publicly accessible and verifiable, it becomes easier to conduct audits, trace fake entries, and track the history of each credential.

By integrating blockchain, smart contracts, and web-based verification, the system provides a scalable, secure, and publicly accessible solution to the problem of certificate forgery. It reduces reliance on manual processes, increases trust in issued documents, and provides stakeholders with a reliable verification mechanism.

User Interaction

The system is designed with a user-friendly interface to accommodate two main types of users: issuers (admins) and verifiers (students, employers, institutions).

Admin Functions:

Login via MetaMask wallet for identity verification.

Upload certificate details like student name, course, institution, date, and certificate ID.

View, manage, and validate the list of certificates added.

Prevent duplicate uploads through smart contract checks.

Verifier Functions:

Enter certificate ID or student name on the public portal.

Instantly check if the certificate is valid and authentic.

View verified certificate details (such as name, institution, and issue date).

Report suspicious or fake certificates through a "Flag for Review" option.

The system ensures smooth and secure interaction between users and the blockchain through a clean web interface integrated with MetaMask.

Security and Traceability Security and traceability are the core strengths of this blockchain-powered verification system:

Immutability: Once data is added to the blockchain, it cannot be changed or deleted. This guarantees that certificate records are tamper-proof and authentic.

Decentralization: The system has no single point of failure. All transactions are stored across multiple nodes on the Ethereum blockchain, ensuring continuous availability even if one node goes offline.

Authentication via MetaMask: Only verified institutions with MetaMask wallet access can issue or upload certificates. This prevents unauthorized users from adding fake entries.

Smart Contract Validation: All actions—such as adding, verifying, or querying certificates—are controlled through smart contracts that enforce strict validation rules.

Transparent Ledger: Every transaction, including certificate uploads and verifications, is publicly recorded. This allows institutions and regulatory bodies to audit and trace all activities, making fraud detection easier.

Technology Stack

VIII. TECHNOLOGY STACK The system uses a modern blockchain-based tech stack for secure and decentralized certificate verification:

Component Technology Used Blockchain Ethereum (testnet: Ganache/Sepolia/Goerli) Smart Contracts Solidity programming language Wallet MetaMask (browser extension for auth) Frontend HTML, CSS, JavaScript, Web3.js Backend Web3-enabled interface + Remix IDE Testing Ganache (local Ethereum blockchain) Integration Web3.js for connecting frontend with contract

This stack allows for easy development, testing, and scaling of the system while maintaining high security and decentralization.

Expected Benefits

Implementing this blockchain-based certificate verification system offers numerous advantages:

High Security: Certificate records are immutable and cryptographically secure.

Real-time Verification: Employers and institutions can verify credentials instantly from the blockchain.

Global Accessibility: Certificate records can be verified from anywhere in the world via the internet.

Prevention of Fraud: Reduces the circulation of fake degrees, mark sheets, and work experience letters.

Audit-Ready: Public ledger allows for institutional and government audits at any time.

No Middlemen Needed: Eliminates the need for third-party background check agencies.

Digital Skill Integration: Encourages institutions to adopt secure digital methods and introduces students to Web3 tools.

This system not only simplifies the verification process but also builds long-term trust among academic institutions, employers, and learners.

IV. Proposed System

The proposed system offers a decentralized and secure method for authenticating certificates through the Ethereum blockchain. It consists of a web-based portal connected to a smart contract deployed on a blockchain network. The system aims to replace traditional centralized and manual verification processes with a trustless, transparent framework.

The system workflow is as follows:

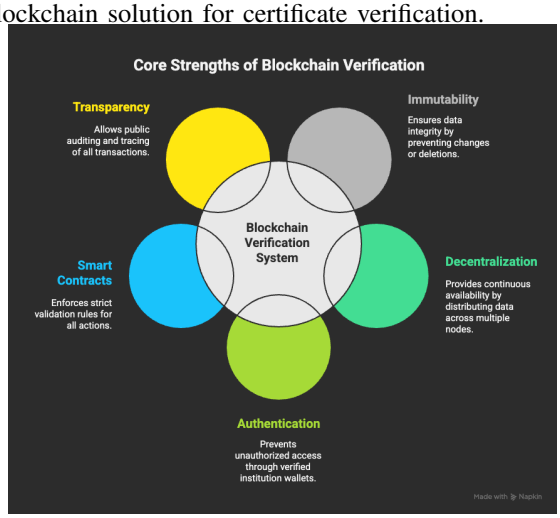
Certificate Issuance by Institutions: Authorized personnel from educational institutions or companies log in using MetaMask for identity verification. Upon successful login, they can upload certificate details such as student name, course, certificate ID, institution name, and date of issue. These details are hashed and submitted to a Solidity-based smart contract.

Blockchain Storage: The smart contract adds this data to a block on the Ethereum blockchain, ensuring that once stored, it cannot be altered or deleted. Each certificate is uniquely linked to its corresponding certificate ID.

User Verification: Employers, students, or third parties can use the web portal to input a certificate ID or name. The system communicates with the blockchain and fetches real-time verification status. A certificate is shown as ”Authentic” if it matches an existing record; otherwise, it is flagged as ”Not Found” or ”Possibly Fake.”

Reporting Mechanism: The system allows users to flag suspicious certificates for review. These flagged entries can be further audited by admin-level accounts or government bodies.

By integrating MetaMask for secure access, smart contracts for automation, and Web3.js for frontend-backend communication, the proposed system delivers a secure and efficient blockchain solution for certificate verification.



V. Results

‘ The proposed system was tested using a simulated Ethereum environment provided by Ganache, allowing for fast, gas-free transactions and thorough testing of all smart contract functionalities.

Dummy certificate data was uploaded successfully through the admin panel.

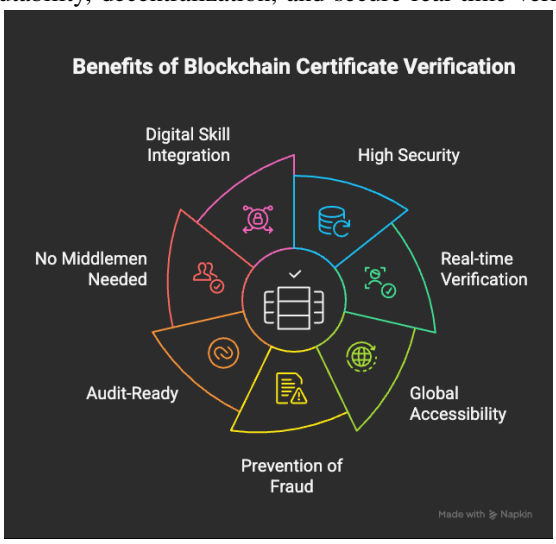
Upon entering a valid certificate ID, the system retrieved all relevant certificate details from the blockchain and marked them as Authentic.

Attempts to upload duplicate or altered certificate data were blocked by the smart contract, confirming the system's resistance to redundancy and tampering.

Invalid or non-existent certificate IDs returned a "Certificate not found" message, enabling quick identification of potential forgeries.

The MetaMask integration worked seamlessly for both admin login and transaction approval, simulating a real-world decentralized authentication process.

These results validated the core system objectives of immutability, decentralization, and secure real-time verification.



VI. Discussion

The successful implementation of the system demonstrates that blockchain can be effectively applied in the field of academic and professional credential verification. Unlike traditional systems that rely on centralized databases, this approach uses the strengths of blockchain—immutability, transparency, and decentralization—to eliminate forgery risks.

One key advantage observed is the system's ability to verify documents without any third-party involvement, saving time for employers and institutions. The blockchain ledger ensures that once data is entered, it remains permanently verifiable, making it ideal for long-term recordkeeping.

However, challenges remain. Gas fees on Ethereum mainnet can be high, which could discourage smaller institutions from adopting the system without subsidies or use of Layer 2 solutions. Furthermore, successful implementation at scale requires collaboration between educational boards, companies, and government bodies.

There is also a learning curve associated with tools like MetaMask and Web3 wallets, which means basic digital literacy training may be necessary for institutional staff. Future upgrades could include user onboarding tutorials and a more intuitive admin panel.

Despite these challenges, the system serves as a scalable and secure foundation for national-level or global adoption.

VII. Conclusion

This research successfully presents a blockchain-based solution to the growing problem of certificate forgery in academic and professional settings. By leveraging Ethereum blockchain, smart contracts, and MetaMask, the system offers a secure, decentralized, and tamper-proof method to issue and verify certificates.

The platform ensures that data cannot be altered post-issuance and allows for real-time verification by any stakeholder through a simple web interface. This eliminates the reliance on centralized authorities and manual validation processes, thus improving efficiency, trust, and transparency.

With further enhancements like mobile QR-based verification, AI-based fraud detection, and DigiLocker integration, this solution has the potential to revolutionize how certificates are managed and verified across educational and professional domains globally.

Acknowledgment

I would like to express my sincere appreciation for the successful completion of this project, which stands as a reflection of consistent research, technical exploration, and a deep interest in emerging technologies. This project allowed me to explore the real-world implementation of blockchain in the field of certificate verification and provided an opportunity to understand decentralized architectures, smart contract development, and secure data storage. The tools and platforms used throughout the development phase—such as MetaMask, Ganache, Remix IDE, and Web3.js—proved essential in transforming conceptual ideas into a practical working system. I am also grateful for the structured academic environment that fostered learning, encouraged experimentation, and supported innovation in applying technology to solve real-world problems like credential forgery and verification delays. This work has contributed significantly to my growth in both technical knowledge and research application.