Enhancing Certificate Validation with Block Chain: A secure and efficient approach

1. Tanu Singh, 2. Birendra Kumar Saraswat, 3. Akash Mishra, 4. Krati Sharma, 5. Vivek Kumar Gupta

1. Computer Science & Engineering Raj Kumar Goel Institute of Technology, Ghaziabad,UP, India
956560tanu@gmail.com

2. Computer Science & Engineering Raj Kumar Goel Institute of Technology, Ghaziabad,UP, India
saraswatbirendra@gmail.com

3. Computer Science & Engineering Raj Kumar Goel Institute of Technology, Ghaziabad,UP, India
Akashmishraa202@gmail.com

4. Computer Science & Engineering Raj Kumar Goel Institute of Technology, Ghaziabad,UP, India
Sharmakrati5393441@gmail.com

5. Computer Science & Engineering Raj Kumar Goel Institute of Technology, Ghaziabad,UP, India
Vivek56official@gmail.com

Abstract:

As more people seek for the education increase day by day, students become more concerned about their careers. As a result, they achieve many certificates. These certificates help them when they apply for jobs in public or private sectors. However, incidents may occur where students generate fake certificates, making it very cumbersome to identify them, in today's time, forging certificates has become a business for many people. Therefore, for many Organizations and institutions Reviewing and verifying certificates has become a boring task. To solve the problem of fake certificates, a digital certificate system based on blockchain technology has been proposed. With the help of blockchain technology, each certificate has a unique hash key that any organization can use to verify its reliability through a portal. Using this technology, we can provide a more secure and efficient system for digital certificate verification. The main goal of this system is to make the certificate validation process very simple.

Keywords:

Blockchain, Certificate, Cryptography, Digital Credentials, Authentication.

I. Introduction

The increasing relevance of educational and vocational certificates in present-day society has also led to a rise in certificate forgery and documentation fraud. Issuing and validating certificates using traditional methods is heavily reliant on centralized systems that are subject to tampering, inefficiencies, and human error. Feeble anti-forge mechanisms sometimes allow deserving individuals and institutions' worth to be tarnished by counterfeit certificates and taking advantage of blockchain technology has proven to be a revolutionizing solution to these problems. Block chain serves as the most transparent and reliable technology as a distributed ledger that is immutable, secure, and decentralized. Implementing block chain for certificate verification will help any educational institution verify its authenticity and preserve its integrity, resulting in elimination of fraud and inefficiencies in certificate verification processes.

Certificate management exploits require centralized repositories, which are susceptible to data loss, unauthorized access, and manipulation. This is compounded by manual validation processes that introduce additional friction: validating against multiple institutions or regions can lead to delays. So, these challenges represent the need for a strong, automated, and decentralized system able to offer secure real-time certificate validation also such problems can be directly solved by a block chain-based certificate validation system that not only redeems the certificates but also keeps the data tamper-free, accessible globally (for real-time validation) and reduces dependency on intermediaries. By leveraging the core principles of block chain technology—decentralization, immutability, and transparency—the solutions will transform the management and verification of certificates. To remove this disadvantage, a technology called blockchain leads us to our lives as a faint light of hope. So why use blockchain? This is because data within the blockchain cannot be changed under realistic conditions. Even if the data changes, it only takes a second to investigate the operation. In blockchain, data or knots are validated only if approved by several parties. Therefore, the system is always reliable and authenticated. This will resolve the operational issues. The next issue that appears in the photo is time-consuming verification. The system you build not only checks the certificate, but also generates the certificate. Everything is automated, so it only takes a few seconds to validate the document. Everything is stored digitally, so students don' t have to worry about losing or damaging their certificates during verification. This proposed system not only removes gaps in the current system, but also provides an effective and concrete solution.

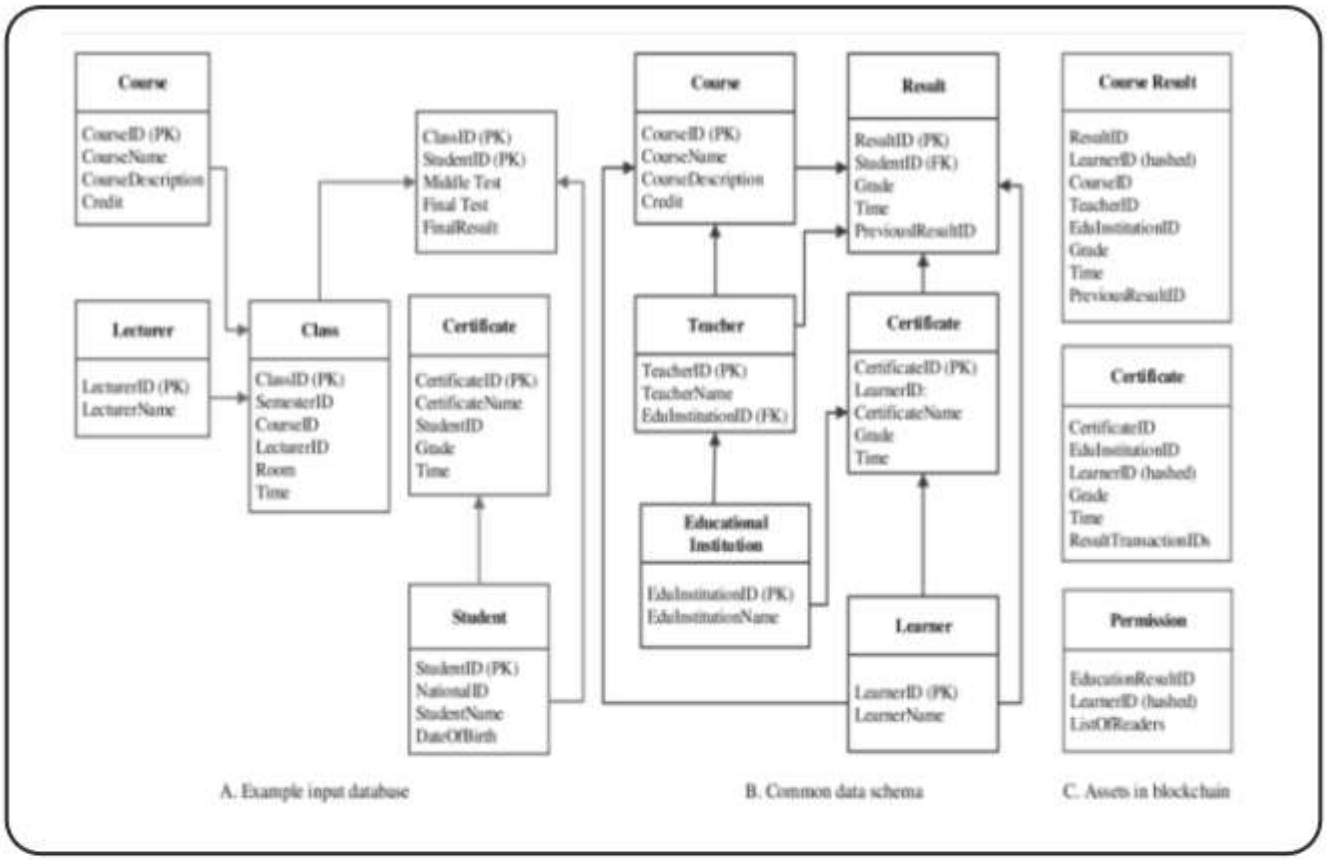

Fig.1: Example of Database in Blockchain

Decentralization: Blockchain eliminates this central dependency by distributing the certificate details across several nodes in the network. This reduces the risk of fraud because it guarantees that the information about the certificate is not controlled or altered by any single entity.

Transparency and Immutability: Once a certificate is put on the blockchain, it cannot be modified or altered. In a way, all transactions or updates about the certificate are stored on the blockchain in a transparent manner so anyone can verify its authenticity. This immutable characteristic ensures that the history of the certificate stays intact, from issuance right through to validation.

Security: Blockchain technology uses cryptographic methods to guarantee the integrity and privacy of the information. The information cannot be tampered with and cannot be faked because certificates are verified by a public-private key pair. In addition, the decentralized characteristic of the blockchain makes it more immune to cyberattacks in comparison to centralized systems.

Automation with Intelligent Contracts: You can also integrate intelligent contracts into smart contracts that include provisions for contracts between all participants on the blockchain platform. Such contracts can automate the certificate verification process, so the criteria for checking certificates are automatically verified without human effort.

Real-Time Verification at Lower Cost: Blockchain ensures instant verification of certificates, thus minimizing time and costs as compared to conventional manual verification methods They provide verification without intermediaries for both employers, colleges, and others.

Improved Privacy: Due to the idea of selective disclosure, only relevant and non-confidential data can be made public without compromising the identity of the entities involved. It keeps it private while still allowing the certificate to be trusted. It utilizes block chain technology to implement certificate, which enhances the credibility, security, and efficiency of validation of any kind of certificates.

II. LITERATURE SURVEY

This project focus on building and immutable certificate generation as well as validation system. In order to achieve this, we have referred few previously publish paper and works of various individual in this field. Our literature survey is mainly based on block chain technology.

C.VinayChowdary et al, V. Sudharshan et al, K. Bhargav et al, Ms. Mounika et al, Ms. Sterlin5 et al [1] Certificate Verification and Validation Using Blockchain in blockchain technology, a decentralized system refers to a network that is not operated by a single organization or authority. This framework provides the transparency, security and theatre- proof case of the data. Since decentralized systems reduce points of failure, censorship and unapproved control, blockchain is particularly geared toward use cases like currency, supply chain management, certificate validation systems.

Chittiprolu Saranya et al, Chittibomma Sai Sindhu et al, Ikkurthi Chandi Priya Dantu Swathi et al, Anne Dhatri, Dr. A. Kalavathi et al [2] Certificate Validation and Verification Using Blockchain It enables the secure and reliable management of digital certificates based on its decentralization, immutability, and cryptographic security principles. The systematic storing of each certificate as a unique record on the blockchain with an associated cryptographic hash makes each record virtually immune to tampering and easily verifiable. Thus, eliminates risks like forgery, unauthorized access, data manipulation.

M Manjunath ,Dr Usha J et al Certificate Validation Using Blockchain Technology [3] Smart contracts are programs that automatically execute agreements based on predefined conditions written in code. Operating on decentralized blockchain networks such as Ethereum they provide transparency, security, and automation. When the conditions are fulfilled, the contract performs automatically without any middleman. This makes it quicker and cheaper than human intervention and reduces the risk of human error. These contracts are used extensively in applications ranging rom financial services to supply chain management to digital identity verification.

Khushal Y. Bheke et al. Aniket R. Misal et al, Nilkanth S Pokharkar et al, Prof. Gunjal T.S et al Digital Certificate Verification Using Blockchain Technology International Journal of Research Publication and Reviews [4] as a peer- to-peer protocol IPFS provides a scalable and efficient way to store distributed files across the network. This very model enables blockchain systems to provide a decentralized storage solution that is efficient, cost effective, and secure. IPFS makes sure that the files are not vulnerable to the single point of failure, unlike traditional centralized storage as it ensures that the data will be available even if part of the network becomes unavailable.

Avni Rustemi, Fisnik Dalipi et al, A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification [5], in this blockchain provides a verifiable distributed ledger with cryptography mechanism to counterfeit academic certificate.

Garima Sethia et al; Sambarapu Namratha et al; Srikanth H et al; Sreeja CS et al, Academic Certificate Validation Using Blockchain Technology [6], it provides an idea about the blockchain that it provides a common sharing platform for storing, accessing document and minimize the overall tim for verification.

Srilatha Puli et al, Safety Alerting System For Drowsy Driver using blockchain, [7], it ensures real-time monitoring and secure data sharing to prevent accidents. This adds a layer of trust and transparency, encouraging drivers to take warnings seriously.

Rohan Hargude et al, Ghule Ashutosh et al, Abhijit Nawale et al, Pro.Sharad Adsure et al, Generating E-Certificate and Validation using Blockchain [8], this system ensures ransparency, trust, and easy access for employers or educational institutions, streamlining the verification process and protecting the integrity of credentials.

A. Bansal et al, B. Kumar Saraswat et al, B. Sharma et al, S. Nayan et al and K. Kathuria et al Extracting and integrating data from unstructured electronic health records for improved analysis and usability.[9] it leads to instant verification, cost effective and efficient, it enhanced privacy and leads to fraud prevention, it can be accessed globally.

Miss. Anjana R. Godse et al, Miss. Prashila P. Mali et al, Prof. N. M. Sawant et al, Certificate Validation Using Blockchain [10] in this it is a secure, tamper-proof and instant verification of credentials. When a certificate is issued its details are recorded on blockchain creating a permanent and immutable record.

Table 1: COMPARATIVE ANALYSIS OF EXISTING RESEARCH ON RECOMMENDATION MODELS

Author	Research Objective	Methodology	Key findings
C. Vinay Chowdary et al. (2024)	Decentralized certificate validation	Blockchain based verification with SHA 256	Enhance security and Fraud Protection
Chittiprolu Saranya et al. (2024)	Blockchain for academic certification	Ethereum smart contracts	Tamper-proof and efficient verification process
M. Manjunatha et al. (2023)	Smart contract-based verification	Decentralized ledger for digital credentials	Automated, real-time verification
Khushal Y. Bheke et al. (2023)	Peer-to-peer certificate authentication	IPFS for distributed storage	Improved scalability and accessibility
Avni Rustemi et al. (2023)	Systematic literature review on blockchain credentialing	Survey of blockchain implementations	Identified key trends and challenges in blockchain-based certification
Garima Sethia et al. (2022)	Academic certificate validation	Blockchain-based smart contracts	Reduces verification time and enhances transparency
Srilatha Puli et al. (2021)	Security enhancements for certificate validation	Blockchain for real-time monitoring	Prevents fraudulent certificate issuance
Rohan Hargude et al. (2021)	E-certificate generation and validation	Decentralized storage & blockchain	Ensures transparency, trust, and easy access
A. Bansal et al. (2023)	Data integration from digital credentials	Unstructured data analysis with blockchain	Reduces fraud and improves data accessibility
Miss. Anjana R. Godase et al. (2024)	Secure and instant certificate validation	Blockchain-based immutability	Prevents tampering and enhances efficiency

Author's Own

III. PROPOSED MODEL

In this model, the certificates are transformed into digital form. In this system the institute and students can register itself. In this system the technology of blockchain is used and this is used for generating hash value. By using the blockchain technology each block has hash value, timestamp, previous hash value and they are connected together. With the help of login id and password of the student a user can verify the certificates. Ethereum has significantly contributed to broadening the potential of blockchain technology beyond just cryptocurrency. Its facilitation of smart contracts, decentralized applications, and tokenization has established it as a key foundation for various industries and applications. From decentralized funding to impossible tokens, supply chains and decentralized identities, the Ethereum effect continues to influence the development of blockchain and decentralized technologies.

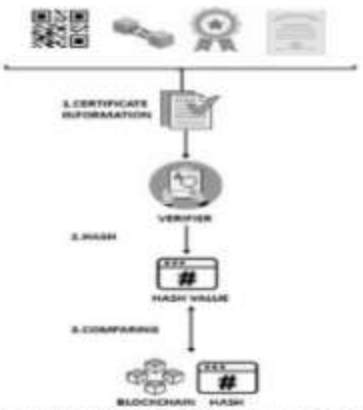

Fig.2: Block diagram of the proposed model

A. Modules

* Blockchain: Blockchain is a common and immutable ledger that allows the process of recording transactions and asset prosecutions across business networks. Create a trusted environment where you can perform actions.
* Ethereum: Ethereum is a decentralized blockchain with small contract capabilities.it is used to pay nodes for performing computational task. In this every action taken happens in the form of transaction on Ethereum blockchain.
* Smart Contract: It is a computer program that automatically execute an agreement between two parties on a blockchain. The code is stored in blockchain, a distributed database that records transaction and cannot be changed.
* Solidity: It is a programming language use to create smart contract on blockchain platform, primarily Ethereum. It has simple syntax similar to that of Java, C++ and Python.
* IPFS: This is a distributed and distributed file storage system to connect all computer devices to the same system or to the same file.
* Nodejs: It is a powerful platform for web development and it is useful to create blockchain application, it increases performance, scalability and easy to use.
* React: It helps to create engaging user interface, it provides reusability of component, fast rendering, code stability, high performance.
* MongoDB: This is a kind of NOSQL database and is used to store details about users and their authentication.

B. Generation of hash value

In order to generate the hash value, The SHA256 algorithm is used for the certificates. It accepts input in various sizes and produces a fixed size hash value. When the hash value generated, the certificate gets uploaded.

C. Validation and Generation at Real Time

Every certificate generated was associated with a unique hash that was stored onto the blockchain. This way if anyone tried to change the certificate it would be immediately obvious since the hash would no longer match up. Traditional systems with their vulnerability for database breaches or unauthorized data alteration would be no match for the proposed system, providing an entirely new answer to data integrity.

D. How Blockchain Works

Blockchain is a distributed and decentralized ledger system designed to ensure secure and transparent record-keeping. This works on a network of nodes (computers) that work together to obtain a synchronous copy of the main register for consistency and reliability. The fundamental building block of this technology is the block, which contains a set of data or transactions, a unique identifier called a hash, and the hash of the previously block to ensure linkage and continuity. When the new transaction happens, it is broadcast to the network, where nodes validate it through consensus mechanisms such as Proof of Work (PoW).

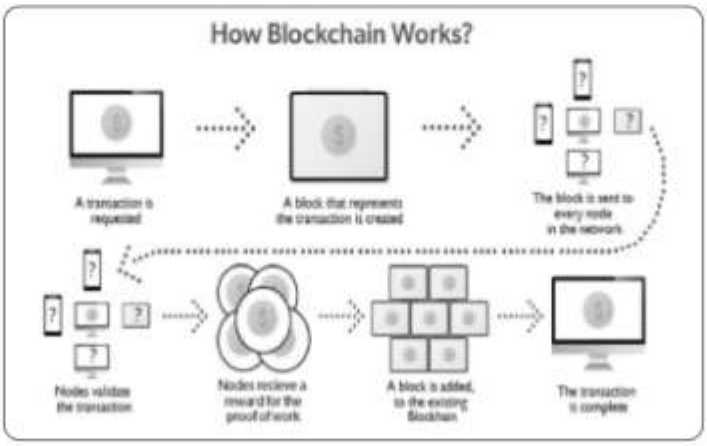

Fig.3: How Blockchain Works

Once validated, the transaction is grouped with others into a block, which is then added to the existing chain in a linear and chronological order. This chain of blocks, secured through cryptographic techniques, makes altering any past
transaction nearly impossible without reworking all subsequent blocks and gaining consensus from the network. Blockchain operates in a decentralized manner, removing the need for intermediaries while improving security and lowering costs. Additionally, its transparency allows all participants to view the ledger, while cryptographic algorithms ensure the data remains

secure, unalterable, and accessible only to authorized individuals. By combining decentralization, cryptography, and consensus, blockchain has emerged as a revolutionary technology that underpins cryptocurrencies, smart contracts, and applications in industries ranging from finance to supply chain management and certificate validation.

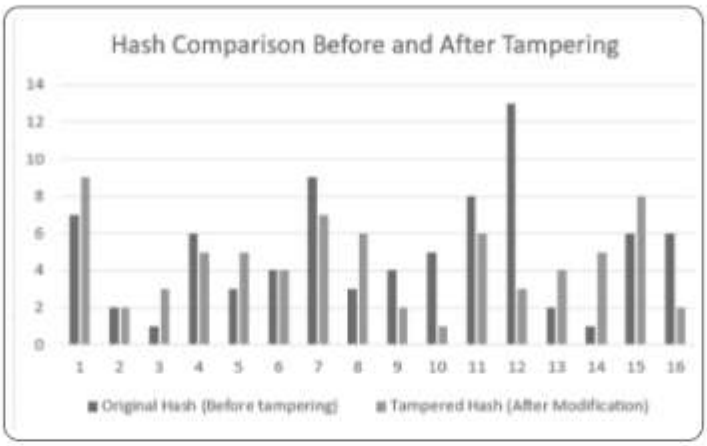

Fig.4: Hash Comparison Before and After Tampering

A. How Blockchain Powers Certificate Validation System

The adoption of block chain technology for certificate validation has revolutionized the process by addressing critical challenges associated with traditional systems. One of the most significant impacts is the drastic reduction in certificate fraud cases. By leveraging block chain's immutability and decentralized nature, organizations can ensure the authenticity of certificates, making it nearly impossible to forge or tamper with credentials. This establishes trust among stakeholders, including educational institutions, employers, and government bodies. Another transformative impact is the reduction in verification time. Traditional certificate verification methods are often manual, time-consuming, and prone to human error. Block chain automates the process through smart contracts, enabling instant and accurate verification. This not only enhances efficiency but also reduces operational costs for organizations. The blockchain based certificate validation system represents a pivotal step towards a transparent, secure and efficient future, setting a new benchmark for digital trust in credential management.

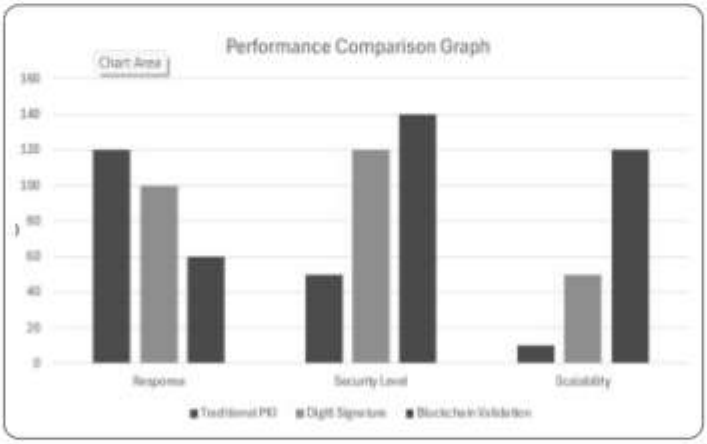

Fig.5: Performance Comparison Graph

IV. RESULTS AND DISCUSSION

It effectively utilizes cryptography hashing to achieve certificate immutability in its blockchain-based system. Every certificate generated was associated with a unique hash that was stored on to the blockchain. This way if anyone try to change the certificate then the hash value would be no longer match up. Traditional system with their vulnerability or database breaches or unauthorize data alteration would be no match for the proposed system providing an entirely new answer to data integrity. The results of this study supported the blockchain-based system's performance in enhancing data integrity and security. The system successfully generated unique cryptographic hashes for each certificate, which ensured immutability, as proven through testing. The system had drawbacks, though, including prohibitively high initial deployment costs as well as a requirement to understand how to implement the blockchain. One drawback was the system's dependence on constant network connectivity, which could be an issue in more remote locations.

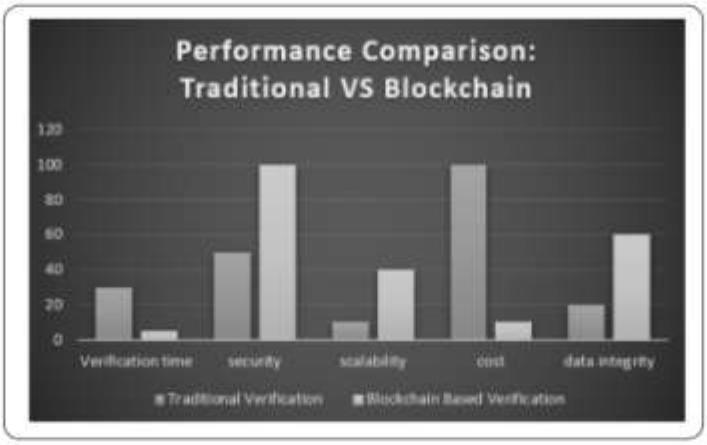

Fig.6: Performance Comparison: Traditional vs Blockchain

A. Validation and Generation at Real Time

A decentralized approach to store and retrieve the certificate using the Inter Planetary file system(IPFS) in parallel with Ethereum blockchain IPFS helped users to store data across the globe enabling better scalability and accessibility as well as reduce reliance on centralized server. This decentralization solved the single point of failure.

B.Addressing Current Challenges

Verification of academic certificates through the traditional method is riddled with challenges of tampering, loss and delays. A blockchain-based solution addressed these challenges through secure, automated and transparent verification procedures. Using immutable and decentralized blockchain technology, the system solved important needs. The integration of blockchain technology into certificate validation has transformed the conventional process of certificate verification. In this approach, institutes upload and authenticate student certificates, while students can securely access the verified certificates shared by their institutes.

- Developed a decentralized application and created a certificate system using a custom blockchain.
- Highlighted the key features of this technology, including its incorruptibility, encryption, traceability, and ability to synchronize data efficiently.

V. Conclusion

This paper presents a solution to combat certificate forgery by utilizing blockchain technology. The focus is on enhancing data security through blockchain's key features, such as immutability and resistance to tampering. Various technological approaches have been explored to minimize certificate fraud while maintaining the security, validity, and confidentiality of academic credentials. Despite certain challenges related to data security and privacy, a blockchain-based system significantly reduces the risk of certificate forgery. The automated certificate issuance process ensures transparency, allowing companies and organizations to verify certificates efficiently. The proposed system lowers management costs, prevents document falsification, and delivers accurate, reliable digital certificate authentication. The block chain-based certificate verification approach proved to offer distinct benefits over centralized approaches in terms of security, efficiency, and scalability with the intent to deceive.

This paper presents a solution to combat certificate forgery by utilizing blockchain technology. The focus is on enhancing data security through blockchain's key features, such as immutability and resistance to tampering. Various technological approaches have been explored to minimize certificate fraud while maintaining the security, validity, and confidentiality of academic credentials. Despite certain challenges related to data security and privacy, a blockchain-based system significantly reduces the risk of certificate forgery. The automated certificate issuance process ensures transparency, allowing companies and organizations to verify certificates efficiently. The proposed system lowers management costs, prevents document falsification, and delivers accurate, reliable digital certificate authentication. The block chain-based certificate verification approach proved to offer distinct benefits over centralized approaches in terms of security, efficiency, and scalability with the intent to deceive.

chain certificate management while also reducing verification applications, illustrating an effective and novel time and cost. Additionally, using blockchain solution to the ongoing challenges of certificate guarantees long-term accessibility and immutability, management. Allowing the records of certificates not to be modified.

REFERENCES

[1] C.VinayChowdary ,V.Sudharshan ,K. Bhargav, Ms.Mounika and Ms. Sterlin5 Certificate Verification and Validation Using Blockchain International Journal of Research Publication and Reviews, Vol 5, no 1, pp 1850-1854 January 2024.

[2] Chittiprolu Saranya, Chittibomma Sai Sindhu, Ikkurthi Chandi Priya Dantu Swathi ,Anne Dhatri,Dr. A. Kalavathi Certificate Validation And Verification Using Blockchain © 2024 JETNR | Volume 2, Issue 4 April 2024 | ISSN: 2984-9276 | JETNR.ORG.

[3]M Manjunatha, Dr Usha J CERTIFICATE VALIDATION USING BLOCKCHAIN TECHNOLOGY Volume:05/Issue:09/September- 2023.

[4] Khushal Y. Bheke,Aniket R.Misal , Nilkanth S.Pokharkar, Prof. Gunjal T. S Digital Certificate Verification Using Blockchain Technology International Journal of Research Publication and Reviews, Vol 4, no 5, pp 3722-3726 May 2023.

[5] Avni Rustemi,Fisnik Dalipi, A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification June 2023 IEEE PP(99).

[6] Garima Sethia; Sambarapu Namratha; Srikanth H; Sreeja C S Academic Certificate Validation Using Blockchain Technology 2022 International Conference on Trends in Quantum Computing and Emerging Business Technologies.

[7] Srilatha Puli, Safety Alerting System For Drowsy Driver using blockchain, 9th International Conference On Innovations In Electronics & Communication Engineering (ICIECE2021), Page- 40.

[8] Rohan Hargude, Ghule Ashutosh, Abhijit Nawale, Pro.Sharad Adsure Generating E-Certificate and Validation using Blockchain www.ijcrt.org © 2021 IJCRT | Volume 9, Issue 7 July 2021 | ISSN: 2320-2882.

[9] A. Bansal, B. Kumar Saraswat, B. Sharma, S. Nayan and K. Kathuria, "Data Extraction and Integration from Unstructured Electronic Health Records," 2023 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS), Tashkent, Uzbekistan, 2023, pp. 1006-1013, doi: 10.1109/ICTACS59847.2023.10390009.

[10] Miss. Anjana R. Godase , Miss. Prashila P. Mali , Prof. N. M. Sawant Certificate Validation Using Blockchain www.ijcrt.org © 2024 IJCRT Volume 12, Issue 4 April 2024 | ISSN: 2320-2882