Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 07, July-2024

Counterfeit Detection of Documents using Blockchain

Dr. Chanchal Antony, Prakruthi S Shetty, Shreya S Shetty, Vaishishta P, Vijeth Kumar
Department of Computer Science and Engineering,
AJ Institute of Engineering and Technology Karnataka, India.

ABSTRACT

Document forgery is a common method that has been used by many people for their own benefits. Document often has its own unique identity which contains a very sensitive content. The current problem related to document is about the document forgery where advanced technology capable in duplicating and modifying a document. The current document verification system often checks for its availability only and does not check for its integrity which is its content. Moreover, current practices provide a low efficiency in detecting a forged document which resulting in false results. Therefore, blockchain will be introduced where it needs to be used to create a new document verification system while integrating with Interplanetary File System (IPFS) to increase the efficiency in detecting a forged document.

Keywords: **Blockchain, Authenticity, Document verification, Inter Planetary File System, Smart Contracts.**

1. INTRODUCTION

Blockchain technology is a digital ledger that functions as a decentralized database, storing data and information throughout a computer system's whole network. The introduction of blockchain technology in the context of cryptocurrencies began in 2006 with the creation of Bitcoin. A cryptocurrency is a form of digital money that can be used to make online purchases and conduct transactions. The distributed ledger used by blockchain technology ensures that every transaction made on the network is secure. This allows other users to verify the legitimacy of a particular transaction. Nowadays, a wide range of industries, including healthcare, banking, inventories, and management, use blockchain technology. The application of blockchain technology has helped to develop a mechanism that will maintain the transactions and safely store the data, making it simpler to find the attacker when blockchain technology is used. Blockchain technology will enable a document verification system to enhance its security features.

Paper documents are typically used to issue documents or other records pertaining to students. These documents can be misplaced or compromised, and they are simple to forge. Blockchain technology is a method of storing data that makes it hard or impossible for hackers to alter or compromise the system. A blockchain is an electronic record of transactions that is distributed and replicated throughout the network of connected computer systems. The certificates that are granted by the organizations are printed documents with easily modifiable information thanks to modern technologies. Both the company issuing the document and the person receiving it are at risk from this. Therefore, it's essential to confirm the record from a reliable source. In order to complete this process, it cross-verifies with the recipient and the organization, which can be costly and time-consuming. Recently, blockchain technology has been applied to fight document fraud and misuse and to enhance the document verification process. The goal of this technology is to prevent the issue of fraudulent documents or phony certifications.

2. RELATED WORKS

Omsar S. Salesh, Osman Ghazali and Muhammad Ehsan Rana, “Blockchain based framework for educational certificates verification”, This paper introduces a system using Hyperledger Fabric for verifying academic certificates. It aims to enhance document verification by assigning unique user IDs, securing data flow via encrypted API endpoints, linking uploaded documents to owners for ownership protection, and ensuring verifier anonymity. This system combats the creation of fake certificates, Verification and validation of Academic Certificates”, A study published in the Annals of Emerging Technologies in Computing (AETiC) by Leka, E. and Selimi, B. describes a blockchain-based application for academic degree.**[1]**

Leka, E. and Selimi, B., 2021. “Development and Evaluation of Blockchain based Secure Application for Verification and validation of Academic Certificates”, A study published in the Annals of Emerging Technologies in Computing (AETiC) by Leka, E. and Selimi, B. describes a blockchain-based application for academic degree verification. With the goal of removing administrative obstacles and improving the

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 07, July-2024

effectiveness and security of the verification process, it distributes, stores, and verifies academic credentials using Ethereum's smart contracts. The application also uses AES encryption to protect the privacy of user data. [AETiC Journal, Volume 5, Issue 2, 2021].**[2]**

Mili Rafi, Sherin Mary Shaji and Prof. Ashly Thomas, "Certificate Management and Validation system using Blockchain", A blockchain-based system for managing and validating certificates was presented by Mili Rafi, Sherin Mary Shaji, and Prof. Ashly Thomas in their paper "Certificate Management and Validation system using Blockchain," which was published in the International Research Journal of Engineering and Technology (IRJET). The administrator, the student, and the verifier are the main players in this system. Using composer Rest Server, all of the student data entered by the administrator is deployed in the hyperledger fabric. The university verifies the preview of the certificate before entering the digital signature. There is a hash code made. Only certified certificates are utilized in the hyperledger. A copy of the certificates is sent to the pupils using QRcodes. The verifier can quickly validate a student's certificate by simply sharing their QRcode with them (Volume 7, Issue 5, May 2020).[3]

Curmi, A. and Inguanez, F., 2018, July "Blockchain based certificate verification platform", developed a prototype for the registration of academic institutions, faculty, and students, as well as the issuance of certificates. Their paper, "Blockchain based certificate verification platform," was published in the International Conference on Business Information Systems (pp. 211-216). An interface is made as a result so that students can get their certificates. Because the certificates are kept on blockchain, third-party verification methods are not necessary. [4]

Clemens Brunner, Fabian Knirsch and Dominik Engel, "SPROFF: A Platform for Issuing and Verifying Documents in a Public Blockchain", Presented at the 5th International Conference on Information Systems Security and Privacy (ICISSP) 2019, Clemens Brunner, Fabian Knirsch, and Dominik Engel wrote "SPROFF: A Platform for Issuing and Verifying Documents in a Public Blockchain." They developed a public blockchain platform called SPROOF for issuing and validating documents. No limitations are placed on the issuer by this platform. All that is recorded to the blockchain within the transaction are the data hashes. Using a key derivation function (KDF), one can produce one or more private keys from a master key. The issuer generates a pair of public and private keys in order to start a new account. To demonstrate to the verifier who owns a document, the public key and its corresponding private key are utilized. In order for the recipient to upload papers to this portal, they must sign up with the issuing organization. A Hierarchical Deterministic Wallet is used for key management. The Web of Trust guidelines are followed by this platform.[5]

ayesh G.Dongre, Sonali M. Tikam, Dr. Kishore.T.Patil and Vasudha Gharat, "Education Degree Fraud Detection and Student Certificate Verification using Blockchain", In their article "Education Degree Fraud Detection and Student Certificate Verification using Blockchain, J" Jayesh G. Dongre, Sonali M. Tikam, Dr. Kishore T. Patil, and Vasudha Gharat suggested that identity document forgery is the process of altering and replicating an authorized identity document for use by an unauthorized party or parties. The article was published in the International Journal of Engineering Research & Technology. They have an abundance of methods and resources that are quite helpful in creating false identities. The study examines current strategies for reducing the danger of document forgery counterfeiting, as well as its advantages and disadvantages. These methods are not enough to stop ID forgeries. New methods and approaches need to be created. A false identity, which is typically created using a combination of real and made-up information, is the foundation of identity theft.**[6]**

A. Gayathiri, J. Jayachitra and Dr.S.Matilda, "Certificate validation using blockchain", Presented in the IEEE 7th International Conference on Smart Structures and Systems (ICSSS 2020), an application was developed to use blockchain technology for certificate validation. Samples and quantization are used to turn paper certificates into digital certificates. The hash value is produced using the chaotic algorithm. The administrator can register students and submit their certificates. The student's certificate can be uploaded by administrators via the admin login, which changes the analog image to a digital one. They can use their Verifier login ID and password to validate their certificate.[7]

Han, M., Li, Z., He, J., Wu, D., Xie, Y.and Baba, A., 2018, September. "A novel blockchain-based education records verification solution", The goal of the Proceedings of the 19th Annual SIG Conference on Information Technology Education (pp. 178–183) is to provide students control over their academic records in a secure setting. By integrating cutting-edge blockchain technologies, this system enables students to collect and distribute certificates to anybody directly, while institutions can give certificates as evidence of accomplishment.[8]

Affandi Husain, Majid Bakhtiari, Anazida Zainal, "Printed Document Integrity Verification Using Barcode", The Journal of Technology and Science, When someone tries to use illegal methods to get what they want, fraud usually results. A sort of fraud known as "document forgery" occurs when someone copies and mimics the unique characteristics of original documents, including the signature and identification number. There are several ways to fake documents, including Print, Copy and Paste (PPC), imitation, Reversed Engineered Imitation (REI), Scan, Edit, and Print (SEP), and others. The main objective of every forgery was to produce an unofficial document that would deceive the authorities or other parties into granting them what they desired, such as entering a country illegally or laundering money, vol. 70:1, p. 99–106, 2014.[9]

Barbara Guidi, Andrea Michienzi, Laura Ricci, "Data Persistence in Decentralized Social Applications: The IPFS approach", The IEEE 18th Annual Consumer Communications & Networking Conference (CCNC), held in Italy in 2021, detailed one method for utilizing the Interplanetary File approach (IPFS) to confirm file integrity. IPFS locates its address, which is a hash of the data, using the content of the data rather than a domain name.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 07, July-2024

An option provided by IPFS is known as "pinning services," which maintains persistent host nodes on a cloud service provider and guarantees that data remains in the network continuously without being automatically deleted.[10]

Muhammad Dhiyaul Rakin Zainuddin and Kan Yeep Choo "Design a Document Verification System Based on Blockchain Technology", (Editor): AER 214, MECON 2022, pp. 229–244, 2023. Blockchain technology provides several characteristics and advantages for creating a system for document verification. IPFS's interaction with the Ethereum blockchain makes it easier to distinguish between modified and original files. The blockchain offers a superior way to store credentials since it records them permanently, protecting any connected information from theft or unauthorized access.**[11]**

Rafah Amer Jaafar PP, Saad Najim Alsaad P. "Enhancing Educational Certificate Verification With Blockchain and IPFS: A Decentralized Approach Using Hyperledger Fabric", TEM Journal. The research proposed a blockchain-based solution to the issue of fake educational certificates. A decentralized architecture for the verification of educational credentials was successfully developed and built using the Hyperledger Fabric platform and IPFS as the decentralized file system. By keeping certificate files on IPFS and only the IPFS hash on the blockchain, the proposed approach offers immutability and reduces the amount of data that needs to be stored there. The system that is being suggested offers several benefits. It significantly lowers the expense and labor required to verify school credentials, Volume 12, Issue 4.**[12]**

Marco Baldi , Franco Chiaraluce, Emanuele Frontoni, Giuseppe Gottardi, Daniele Sciarroni, and Luca Spalazzi "Certificate Validation through Public Ledgers and Blockchains", proposed a blockchain-based PKI solution in the Proceedings of the First Italian Conference on Cybersecurity (ITASEC17), Venice, Italy, to address the security and reliability issues with certificate revocation information. Its main benefits are that it can be implemented using existing open source platforms with relative ease and does not require a single POF. The risk of security breaches brought on by a lack of current and real-time information regarding revoked certificates is decreased by the distributed and resilient structure of blockchains.**[13]**

Anthonya, Michael Christian Leea, Rafaelle Richel Pearla, Ivan Sebastian Edberta, Derwin Suhartono "Developing an anti-counterfeit system using blockchain technology", presented at the 7th International Conference on Computational Intelligence and Computer Science 2022, with a publication number of 1877-0509, suggested a distribution method based on blockchain technology to counteract counterfeiting. Using this approach would guarantee that every product in the system is authentic.**[14]**

Vipul Badhe, Pooja Nhavale, Sonal Todkar, Prajakta Shinde, Prof. Kiran Kolhar "Digital Certificate System for Verification of Educational Certificates using Blockchain", published in the International Journal of Science and Technology Research Publications. Despite numerous limitations regarding data security and privacy, a number of strategies have been investigated to lessen the likelihood of certificate forgeries and ensure the security, authenticity, and confidentiality of graduation certificates. A novel blockchain-based method lowers certificate forgery. The automatic certificate issuance process of the system is transparent and open. Thus, businesses or organizations can ask the system for details regarding any certificate, Volume 7, Issue: September-October, 2020; ISSN: 2395-6011.[15]

3. BLOCKCHAIN TECHNOLOGY CHARACTERISTICS

Blockchain technology uses many other techniques to counterfeit the documents like distributed consensus algorithms, cryptography and mathematics. Blockchain technology has six characteristics and they are as follows:

are guaranteed by consensus mechanisms like Proof of Work (PoW), Proof of Stake (PoS), and others. Furthermore, the network's decentralized structure makes it more resistant to cyberattacks.

1. Decentralization: The primary characteristic of blockchain technology is its decentralized architecture. Every node in the distributed network that powers it has a copy of the whole blockchain. This increases openness and lowers the possibility of a single point of failure by doing away with the requirement for a central authority or middleman.
2. Immutable and Tamper-Resistant: Because of cryptographic hashing and the consensus process, data stored on the blockchain is very difficult to change or remove. Because of its immutability, network users may trust one another and the data's integrity is guaranteed.
3. Transparency: Blockchain provides a publicly viewable, transparent ledger where all network users can see all transactions and data entries. Since everyone can confirm the data stored on the blockchain, this transparency promotes confidence.
4. Security: Blockchain protects data and transactions with cryptographic methods. The validity and security of transactions

5. Consensus Mechanisms: Blockchain consensus protocols ensure network-wide agreement on data or transactions. Protocols like Proof of Work, Proof of Stake, Delegated Proof of Stake maintain uniformity across nodes regarding the blockchain's current state.
6. Smart contracts: are self-executing agreements that have the provisions of the contract explicitly encoded into the code. When certain criteria are met, these contracts automatically enforce and carry out preset activities, reducing the need for middlemen and increasing efficiency.
7. Distributed Ledger: A copy of the ledger is stored on each blockchain node in the network. Because the network is spread, even in the event of a node failure or breach, the availability and integrity of the data are preserved.

4. PROPOSED SYSTEM

4.1 Methodology

Store document hashes and metadata on a blockchain for accessibility and transparency while protecting original content by using cryptographic fingerprints. Access control and verification are automated using smart contracts. Document hashes are validated through authentication by comparing stored hashes to ones supplied. Use QR, NFC, or RFID codes to effectively authenticate users. Consistent audits and the use of new technologies strengthen defenses against intrusions, verifying the legitimacy of documents through blockchain.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 07, July-2024

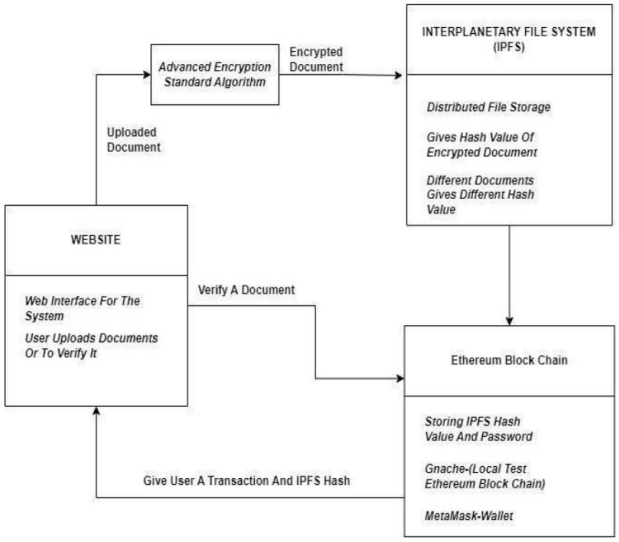

Fig. 1. Architecture of the proposed system

4.2 Objectives

The immutable feature of the blockchain provides greater security and transparency in the transactions of the proposed system, which issues digital certificates with more accurate information without the involvement of a third party. This eliminates the need for the current technologies, where certificates are issued on paper and must be validated by human resources, which takes more time.

5. APPLICATIONS

Supply Chain Management: Companies use blockchain to track and verify the authenticity of documents related to the supply chain, preventing counterfeiting of products and ensuring transparency.

Digital Certificates: Educational institutions issue diplomas and certificates on the blockchain, making it easy to verify their authenticity and eliminate the risk of counterfeit credentials.

Notarization Services: Blockchain-based notary services provide secure and tamper-proof documentation, preventing the forgery of legal documents such as contracts, wills, and property deeds.

Identity Verification: Governments explore blockchain for identity documents like passports or national IDs. Storing this information on a blockchain enhances security and makes it more challenging for counterfeiters to produce fake IDs.

Art and Luxury Goods Authentication: Blockchain is used to verify the authenticity of high-value items like art pieces and luxury goods. By recording ownership and transaction history on the blockchain, it becomes more difficult to create counterfeit versions.

Pharmaceuticals Traceability: Blockchain helps in tracking and authenticating pharmaceuticals throughout the supply chain. This ensures that consumers receive genuine medications and reduces the risk of counterfeit drugs entering the market.

Cross-Border Transactions: International trade and financial documents benefit from blockchain to prevent fraud in cross-border transactions. Blockchain provides a transparent and secure way to verify the legitimacy of trade-related documents.

Secure Digital Voting: Some voting systems use blockchain to secure and verify the authenticity of digital votes, reducing the risk of counterfeit votes or tampering in elections.

4. CONCLUSION

In this work, we put forth a blockchain-based solution to the certificate forgery problem. Ensuring data security is a critical task. Through the utilization of blockchain's unchallengeable quality, we may enhance data security and minimize certificate forgery. The user can view and validate the certificate using the application.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 13 Issue 07, July-2024

REFERENCES

1. Omsar S. Salesh, Osman Ghazali and Muhammad Ehsan Rana,"Blockchain based framework for educational certificates verification",Journal of Critical Reviews, Volume-7, Issue-3, 2020.
2. Leka, E. and Selimi, B., 2021. Development and Evaluation of Blockchain based Secure Application for Verification and validation of Academic Certificates. Annals of Emerging Technologies in Computing (AETiC), 5(2), pp.22-36.
3. Mili Rafi, Sherin Mary Shaji and Prof. Ashly Thomas, "Certificate Management and Validation system using Blockchain", International Research Journal of Engineering and Technology (IRJET), Volume- 7, Issue-5, May 2020.
4. Curmi, A. and Inguanez, F., 2018, July. "Blockchain based certificate verification platform". In International Conference on Business Information Systems (pp. 211-216). Springer, Cham.
5. Clemens Brunner, Fabian Knirsch and Dominik Engel, "SPROFF: A Platform for Issuing and Verifying Documents in a Public Blockchain", 5th International Conference on Information Systems Scurity and Privacy (ICISSP) 2019.
6. Jayesh G.Dongre, Sonali M. Tikam, Dr. Kishore.T.Patil and Vasudha Gharat, "EducationDegree Fraud Detection and Student Certificate Verification using Blockchain", International Journal of Engineering Research & Technology, ISSN, Volume-9, Issue-7, July 2020..
7. A. Gayathiri, J. Jayachitra and Dr.S.Matilda, "Certificate validation using blockchain", IEEE 7th International Conference on Smart Structures ans Systems ICSSS 2020.
8. Han, M., Li, Z., He, J., Wu, D., Xie, Y.and Baba, A., 2018, September. "A novel blockchain-based education records verification solution". In Proceedings of the 19th annual SIG conference on information technology education (pp.178- 183).

9. Han, M., Li, Z., He, J., Wu, D., Xie, Y.and Baba, A., 2018, September. "A novel blockchain-based education records verification solution". In Proceedings of the 19th annual SIG conference on information technology education (pp.178- 183).
10. Han, M., Li, Z., He, J., Wu, D., Xie, Y.and Baba, A., 2018, September. "A novel blockchain-based education records verification solution". In Proceedings of the 19th annual SIG conference on information technology education (pp.178- 183).
11. Han, M., Li, Z., He, J., Wu, D., Xie, Y.and Baba, A., 2018, September. "A novel blockchain-based education records verification solution". In Proceedings of the 19th annual SIG conference on information technology education (pp.178- 183).
12. Rafah Amer Jaafar PP, Saad Najim Alsaad P. "Enhancing Educational Certificate Verification With Blockchain and IPFS: A Decentralized Approach Using Hyperledger Fabric", TEM Journal. Volume 12, Issue 4.
13. Marco Baldi , Franco Chiaraluce, Emanuele Frontoni, Giuseppe Gottardi, Daniele Sciarroni, and Luca Spalazzi "Certificate Validation through Public Ledgers and Blockchains" .In Proceedings of the First Italian Conference on Cybersecurity (ITASEC17), Venice, Italy.
14. Anthonya, Michael Christian Leea, Rafaelle Richel Pearla, Ivan Sebastian Edberta, Derwin Suhartono "Developing an anti-counterfeit system using blockchain technology" published in 7th International Conference on Computer Science and Computational Intelligence 2022, ISSN - 1877-0509.
15. Vipul Badhe, Pooja Nhavale, Sonal Todkar, Prajakta Shinde, Prof. Kiran Kolhar "Digital Certificate System for Verification of Educational Certificates using Blockchain" published in International Journal of Scientific Research in Science and Technology, ISSN: 2395-6011, Volume 7, Issue : September-October-2020.