IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 3, March 2024

DOI: 10.17148/IARJSET.2024.11350

DocBlock: Blockchain based document storage and authentication system

Mr. Sachin Dighe[1], Aditya Mehta[2], Bhaveshsingh Rathod[3], Rishabh Mishra[4]

Assistant Professor, Computer Engineering, Sinhgad Institute of Technology and Science, Pune, India[1]

Student, Computer Engineering, Sinhgad Institute of Technology and Science, Pune, India[2-4]

Abstract: The proliferation of digital documents necessitates the development of secure and reliable methods for their storage and authentication. This paper explores a novel system that leverages blockchain technology to address these challenges and create a robust document management solution. By harnessing the core strengths of blockchain, namely its immutability, tamper-proof nature, and distributed ledger architecture, the proposed system ensures the secure storage and verifiable authenticity of documents. Documents are uploaded in a hashed format, generating a unique fingerprint that guarantees data integrity and prevents unauthorized modifications. Furthermore, access control mechanisms are implemented to restrict unauthorized access and ensure data security. To provide non-repudiation of document origin and prevent forgery, cryptographic signatures are employed, allowing users to verify the authenticity of documents and identify their creators. This blockchain-based system offers several advantages over traditional document management approaches. It significantly enhances security by offering a tamper-proof and immutable record of all documents and their associated actions. Additionally, the system promotes transparency by providing a clear audit trail for all document interactions, fostering trust and accountability. Finally, the distributed nature of blockchain technology eliminates the need for a central authority, streamlining document management processes and reducing reliance on third-party verification. Overall, this paper presents a compelling solution for secure document storage and authentication, offering significant benefits for various sectors that rely heavily on digital documentation.

I. INTRODUCTION

The digital age has ushered in a paradigm shift in document management. Traditional paper-based systems are increasingly being replaced by their digital counterparts, offering numerous advantages such as ease of access, efficient storage, and faster retrieval. However, the digital realm also presents unique challenges regarding document security and authenticity. Unlike physical documents, digital files can be easily modified, replicated, or even forged, raising concerns about data integrity and verification. This necessitates the development of robust solutions that can ensure the security and trustworthiness of digital documents.

Blockchain technology, with its core principles of immutability, transparency, and decentralization, has emerged as a promising candidate for addressing these challenges. A blockchain is essentially a distributed ledger technology that maintains a continuously growing list of records, called blocks, securely linked together using cryptography. Each block can contain various types of data, including document hashes or metadata. Once a block is added to the blockchain, it becomes incredibly difficult to alter, as any modification would require changing all subsequent blocks, which requires the consensus of the entire network. This inherent tamper-proof nature makes blockchain ideal for storing document hashes, which act as unique fingerprints that can be used to verify the integrity of the original document.

In this paper, we propose a novel document storage and authentication system that leverages the power of blockchain technology. Our system utilizes a permissioned blockchain, offering enhanced security and control compared to public blockchains. Documents are uploaded and stored off-chain, with only their cryptographic hashes recorded on the blockchain. This approach ensures data privacy while still benefiting from the blockchain's tamper-proof record-keeping capabilities.

To further enhance security and prevent unauthorized access, we explore the integration of access control mechanisms within the system. These mechanisms can be implemented using various programming languages and frameworks, such as Java Server Pages (JSP) for server-side scripting. Additionally, advanced techniques like facial recognition using libraries such as faceknn in Python can be employed to restrict document access based on user identification. The following sections will delve deeper into the system architecture, its functionalities, and the specific integration of these technologies to create a secure and reliable document management solution.

II. RECOGNIZE THE PROBLEM

The conventional method of storing the documents is using the papers and folders or atmost a electronic device in pdfs or as a picture of the document. But the conventional methods has to much dependence on the availability of the device storing the document, this things limitation was overcome with the introduction of cloud services, now as the availability of data increased so did the threat of data being stolen. The old methods of document storing and handling had many drawbacks such as reduced availability, high risk of data theft, increased number of document forgery along with others. It became difficult to not only track the forged document but also to recognize the original one.

The need for Blockchain based document based storage and authentication system is now more than ever, The advanced technology of blockchain can be used for storing the document safely and in a secure way so that it cannot be forged and used in a way that is not appropriate. The use of various different technologies will make this project a next gen document storage system.

III. LITERATURE REVIEW

Over the past few years, blockchain technology has gained significant traction across various industries. Numerous studies and investigations have explored the potential of integrating blockchain into diverse sectors. This section delves into existing research on how blockchain can be leveraged for document authentication.

[1] In their study, Xingxiong Zhu. (2019) explored the benefits of cryptographic key pairs private and public keys for verifying the authenticity of digital documents. Furthermore, They investigated that the broader applicability of blockchain technology in various domains, including the Internet of Things for data tracking, supply chain management, property registration, and document protection. Significantly, the authors underscored blockchain's capacity to bolster trust in the financial realm through the facilitation of secure credit reporting mechanisms.

[2] Leible and colleagues explored the potential and advantages of integrating blockchain into open science platforms. Their work explored the various sectors that could benefit from blockchain implementation and assessed the impact of blockchain on different industries thus far.

[3] To mitigate potential societal risks, Shah et al. (2019) proposed a theoretical framework for verifying academic certificates using blockchain technology. Their model integrates encryption techniques with private and public keys, alongside digital signatures with timestamping functionalities for verifying digital certificates. Authors delineated a system for issuing and authenticating birth certificates via blockchain.

[4] Blockchain emerges as an advanced technology offering heightened convenience and security compared to centralized data storage systems. In this paradigm, information is not stored in a single location but rather replicated across a network of interconnected computers, each acting as an independent database node. This peer-to-peer network ensures tamper-proof data management. Modifications to any record (block) necessitate altering all subsequent blocks, as each block cryptographically references the previous one using a secure hash function. Additionally, each node or block undergoes encryption using robust hash algorithms, with every block storing the hash code of its predecessor, establishing a continuous chain of interconnected blocks within the network. Given blockchain's increasing global traction owing to its distributed and decentralized characteristics, Joshi and colleagues conducted a comprehensive survey centered on the fundamental hurdles and prospects in blockchain technology. Their work investigated the fundamental challenges and opportunities associated with blockchain technology, while also delving into security and privacy considerations.

[5] The digital revolution has demonstrably enhanced record-keeping security and streamlined administrative processes by reducing time and effort required for maintenance.However, despite these advancements in security, instances of fraud persist, as exemplified by recent incidents such as the discovery of fake birth certificate schemes in Delhi, India.

[6] Zhu, X., & Fan, T propose a user authentication model that leverages multidimensional biometric and behavioral features. This approach utilizes real-time feedback technology based on a user's dynamic behavioral characteristics to detect and authenticate user activity on their terminal device. By analyzing and processing the interactive behavioral data collection, analysis, and processing, a network identity system grounded in legal identity is established.

[7] Traditional identity authentication methods employed in e-commerce, financial services, and energy sectors often rely on single-factor approaches such as passwords or basic biometrics. These methods are susceptible to hacking attempts, data breaches, and lack robust security measures. A significant vulnerability of traditional biometric

DOI: 10.17148/IARJSET.2024.11350

authentication lies in the static nature of biological characteristics, which remain largely unchanged throughout a person's life. In the event of a leak or a system compromise by hackers, information security risks are significantly heightened. These traditional systems face limitations in data security and lack intelligent authentication mechanisms.

[8] The need for a secure, tamper-proof, and easily maintainable data storage solution for birth records is paramount. Existing literature explores the potential of biometric techniques as a preferred method for establishing individual identity. Biometrics leverage unique biological characteristics for authentication, offering an advantage over traditional methods like passwords, PINs, smart cards, keys, and tokens.However, conventional authentication methods like PINs and passwords pose challenges due to their susceptibility to being forgotten or hacked, potentially compromising our physical security. Similarly, there are risks associated with smartcards, keys, and tokens, as they may be lost, stolen, or misplaced, leading to various security concerns. While magnetic stripe cards are susceptible to degradation and data loss, traditional biometric authentication methods, like fingerprint scans, may exhibit slight variations over time, limiting their feasibility for birth certificate security. To address these limitations, this study proposes a more efficient and secure approach for birth certificate storage using blockchain technology and the InterPlanetary File System. This novel system facilitates effortless verification and authentication of birth certificates.

IV. PROBLEM DEFINITION

The tradition document verification method is centralised authorities which can be time consuming and costly ,prone to fraud and lack of transparency and Current centralized systems often require reliance on third-party intermediaries, resulting in delays, higher costs, and risks of data breaches which intend to explore the solution for these issue The project seeks to explore how blockchain cab be leveraged to explore the underlining issue which are as follows Design a secure and tamper proof verfication method,develop efficient mechanism for ownership control and to enhance transparent and traceability in document usage and issuance.

V. OBJECTIVE

The primary objective of the project as follows:

1. Enhance Security: Implement a blockchain-based system to enhance the security of document verification and authentication processes, minimizing the risks of fraud, data manipulation, and un authorized access.
2. Ensure Transparency: Create a transparent and immutable ledger of document transactions to provide stakeholders with verifiable proof of authenticity and integrity.
3. Reduce Costs: Develop a cost-effective solution by eliminating the need for intermediary institutions and reducing administrative overheads associated with document verification processes.
4. Improve Efficiency: Streamline document verification processes by leveraging blockchain technology to automate authentication procedures, reducing processing times and enhancing overall efficiency.
5. Enable Traceability: Enable traceability of document transactions through the blockchain, allowing stakeholders to track the provenance and history of documents throughout their lifecycle.
6. Ensure Privacy: Implement privacy-enhancing features such as encryption and selective disclosure mechanisms to safeguard sensitive information while maintaining transparency and auditability.
7. Provide Redundancy and Disaster Recovery: Implement robust redundancy and disaster recovery mechanisms to ensure the availability and integrity of document records in the event of network disruptions or system failures.

VI. FUTURE SCOPE

The future scope for document verification and authentication using blockchain is vast and promising. Here are some potential areas of future development and expansion:

1. Integration with Emerging Technologies: Explore integration with emerging technologies such as artificial intelligence (AI), machine learning (ML), and Internet of Things (IoT) to enhance the capabilities and functionalities of blockchain-based document verification systems. For example, AI-powered algorithms could be utilized for advanced document analysis and verification, while IoT devices could provide real-time data for enhanced document authenticity.

2. Cross-Industry Applications: Expand the use cases of blockchain-based document verification beyond traditional sectors such as finance and legal to other industries including healthcare, supply chain management, real estate, education, and government services. Each industry presents unique opportunities for streamlining processes, reducing fraud, and improving trust through blockchain technology.

DOI: 10.17148/IARJSET.2024.11350

3. Decentralized Identity Management: Explore the potential for using blockchain as a foundation for decentralized identity management systems, allowing individuals to maintain control over their personal data and digital identities while securely verifying and sharing documents across various platforms and services.

4. Regulatory Frameworks: Work closely with regulatory authorities and policymakers to establish clear and supportive regulatory frameworks for blockchain-based document verification systems, addressing legal and compliance requirements while fostering innovation and adoption in the industry.

5. User-Centric Design: Prioritize user-centric design principles in the development of blockchain-based document verification solutions, focusing on enhancing usability, accessibility, and user experience to encourage widespread adoption among individuals and organizations.

6. Enhanced Privacy Features: Continue research and development efforts to enhance privacy features and techniques within blockchain networks, such as zero-knowledge proofs, ring signatures, and secure multi-party computation, to ensure the confidentiality of sensitive document information while maintaining transparency and auditability

VII. CONCLUSION

In the conclusion survey paper comprehend the application of blockchain technology in document verification and authentication holds immense potential to revolutionize the way we handle sensitive information, ensure trust, and streamline processes across various industries. By leveraging the inherent features of blockchain, including decentralization, immutability, and transparency, we can address longstanding challenges associated with traditional methods of document verification.

Through the development of robust, user-friendly blockchain-based solutions, we have the opportunity to enhance security, reduce costs, and improve efficiency in document management processes. Moreover, by prioritizing interoperability, scalability, and privacy, we can create a framework that not only meets regulatory requirements but also fosters widespread adoption among businesses, governments, and individuals. As we continue to explore emerging technologies, refine regulatory frameworks, and collaborate across industries, the future scope for blockchain-based document verification remains promising. By embracing innovation, fostering community engagement, and prioritizing user-centric design, we can unlock new opportunities for trust, transparency, and collaboration in the digital age.