International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

1

A Blockchain-Based Digital Notary System Provides Reliable and Tamper-Proof Timestamping and Verification Services for Digital Documents: A Review

Deeksha Uikey[1], Dr. Raju Brarskar[2], Dr. Manish Ahirwar[3]

[1]Student, Department of Computer Sciencev & Engg. , University Institute Of Technology , Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal (M.P.), India
[2,3]Associate Professor, Department of Computer Science & Engg. , University Institute Of Technology , Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal (M.P.), India

ABSTRACT
In this paper,we discuss on A blockchain-based digital notary system aimed at enhancing the reliability and security of timestamping and verification services for digital documents. Leveraging the decentralized and immutable nature of blockchain technology, the system offers a tamper-proof solution to authenticate the integrity and existence of digital files. Through cryptographic hashing and consensus mechanisms, timestamps are securely recorded on the blockchain, ensuring irrefutable proof of document existence at specific points in time. The system provides users with a transparent and decentralized platform for verifying the authenticity of digital documents, mitigating risks associated with fraud and manipulation..

Keywords: Legal Service, Electronic Service, Blockchain,Digital Notary System Etc.

1. INTRODUCTION

In an era where digital documents are ubiquitous and the need for secure verification and timestamping is paramount, the emergence of blockchain technology has brought forth innovative solutions. One such solution is the implementation of a blockchain-based digital notary system, offering reliable and tamper-proof timestamping and verification services for digital documents.

Traditionally, notarization has been a crucial process for validating the authenticity and integrity of physical documents. However, the transition to digital documentation has presented challenges in ensuring the same level of trust and security. This is where blockchain technology, renowned for its decentralized and immutable nature, steps in to revolutionize the notary process.

A blockchain-based digital notary system operates on the principles of distributed ledger technology, where information is securely stored across a network of nodes, ensuring transparency and accountability. Each document submission is timestamped and cryptographically sealed into blocks, forming an unalterable chain of records.

About digital Notary system

A digital notary system is a modern approach to the traditional notarial process, which involves verifyi-

ng the authenticity of documents, signatures, and transactions. Unlike the conventional method that relies on physical stamps and signatures, a digital notary system utilizes cryptographic techniques and digital signatures to ensure the integrity and authenticity of electronic documents and transactions.

A trusted entity, often referred to as a digital notary or a trusted third party, employs cryptographic algorithms to create a unique digital signature for each document or transaction. This digital signature serves as a tamper-evident seal, indicating that the document has not been altered since it was signed and attested by the digital notary. Additionally, the digital signature can be verified by anyone with access to the appropriate cryptographic keys, providing a reliable method for confirming the document's authenticity.

Include extra features like time-stamped, which keeps track of the precise moment the transaction or documents is signed. Understanding the chronological sequence of events and settling disagreements over the timeliness of transactions or agreements depend heavily on this time-stamped feature.

This system's resilience to fraud and manipulation is one of its main features. It is nearly hard to change or remove a piece of paper form the blockchain with no the approval of the vast majority of network users. Stakeholders may now be quite confident about the integrity of their digital assets. Furthermore, there is no single point of failure because to blockchain's decentralised architecture, which reduces the possibility of data loss or manipulation. By providing consumers with a safe platform for timestamping and certification with no having to look for middlemen, this improves the notary service's dependability.

Furthermore, by expediting the notarization process, blockchain-based digital notary solutions provide effectiveness and convenience. Both people and corporations may save time and resources by submitting and verifying documentation in a secure and timely manner.

The advent of blockchain computing has made it possible to create digital notary systems that are trustworthy and reliable. Through the use of the intrinsic characteristics of blockchain, namely its decentralisation and immutability, these systems offer a dependable means of timestamping and authenticating digital documents, guaranteeing their authenticity and safety in an ever-more digitalized society.

1.1 Types Of Notary Services Provided By Blockchain

Blockchain technology has the potential to impact three key aspects of notary services.

Using blockchain technology, these provided services cannot directly replace notary services, as stated by the law (at least, not yet); they can only enhance the whole process. From country to country, they could be either accepted or denied.

Highlighted below are the areas where blockchain technology can help with notary public services.

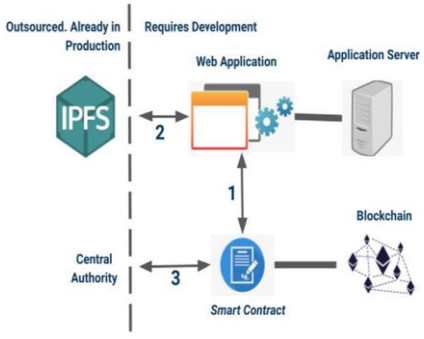

Fig 1 Blockchain and smart contract architecture for notaries services

Blockchain technology has introduced innovative ways to provide notary services, offering solutions that enhance security, transparency, and efficiency in document authentication. Here are some types of notary services provided by blockchain:

- **Digital Signatures**: Blockchain platforms enable the use of digital signatures for documents. Because these signatures are unchangeable and cryptographically safe, they offer a trustworthy way to confirm the legitimacy and consistency of documents.
- **Timestamping**: Document timestamping, or logging the time and date a document was generated or updated, is possible using blockchain technology. This timestamp serves as unquestionable proof of the document's existance at a certain point in time and is recorded in the blockchain's unchangeable ledger.
- **Smart Contracts**: Self-executing contracts, or smart contracts, have the conditions of the contract explicitly encoded into the code. Smart contracts are used by blockchain-based attestation services to organise and enforce the conditions of agreements, such as real estate transactions or legal contracts, eliminating the need for middlemen.
- **Proof of Existence**: Blockchain can be used to create a proof of existence for documents. By hashing a document and storing the hash value in the blockchain, users can prove that a document existed at a particular time without revealing its contents. This is useful for intellectual property rights, patents, and copyright protection.
- **Document Verification**: Blockchain-based notary offices allow users to compare the cryptographic hashes of documentation with entries in the blockchain ledger in order to confirm the legitimacy of the documents. This makes traditional notary services unnecessary and offers a more reliable and affordable way to verify documents.
- **Chain of Custody**: Blockchain can track the chain of custody for important documents or assets, providing a transparent and immutable record of their ownership and transfer history. This is particularly useful in industries such as supply chain management, real estate, and intellectual property.
- **Decentralized Autonomous Organizations (DAOs)**: DAOs are organizations run by smart contracts on a blockchain, with decisions made by consensus among members. Blockchain-based notary services can leverage DAOs to create decentralized and autonomous entities for managing legal or business processes, such as voting on contract disputes or verifying identity.
- **Cross-Border Transactions**: Blockchain-based notary services are designed to make cross-border transactions easier by offering a transparent and safe system for document and agreements verification across countries. This lowers the expense and difficulty of conducting business internationally and navigating the legal system.

2. LITERATURE REVIEW

At present times, the user wants faster data transmission speed and secure services. 5G NR promise to deliver all the basic as well as advanced facilities in contrast to prior. This technology allows users to high-definition and volume data within a second. 5G Technology 5G can handle larger traffic to cover the massive demand of the devices. 5G NR uses mmWave, tiny cells, massive MIMO, beamforming, and full-duplex to achieve this goal. These technologies, however, remain in their infancy and have not been verified.

Jiahao Zhao et.al. (2024):- The consistent rise in transaction volume poses a considerable challenge to blockchain storage capacity. To mitigate this pressure, leveraging cross-chain technology to distribute data across multiple blockchains can alleviate storage constraints significantly. However, the inherent immutability of blockchains may hinder their evolution, as certain outdated identity records, for instance, cannot be modified due to this immutability feature. The decentralized chameleon hash function presents a potential solution, preserving decentralization while allowing for updates to immutable data. Nonetheless, ensuring the consistency of dynamic data updates in cross-chain interactions remains an unresolved concern worthy of further exploration.

Monther Aldwairi et al. (2023):-

We introduce a blockchain-powered credential validation system, where issuing entities create digital certificates stored within a public but permissioned blockchain accessible for verification by students and relevant parties. Our paper provides a comprehensive exploration and formal assessment of this proposed system. Furthermore, we have developed a prototype supporting three distinct use cases. Through formal analysis, our system demonstrates resilience against various common attacks while exhibiting outstanding performance metrics, including CPU and memory utilization, as well as minimal latency in blockchain programming and querying processes.

Lei Shang et al., (2023):- the rapid development of the digital economy, in judicial practice, the type of evidence is developing from physical evidence to electronic evidence. Compared with traditional physical evidence, electronic evidence is vulnerable to external network attacks and tampering by internal practitioners in the process of collection, fixation, storage, transmission, etc. Therefore, determining the authenticity of electronic evidence is costly and difficult to admit, which directly affects the proportion of electronic evidence admissible in litigation. The unique characteristics of blockchain technology, such as tamper-proof, traceability, and multi-party participation, naturally fit with the demand for electronic data deposition. The electronic data deposit based on blockchain technology can avoid evidence forgery and reduce the impact of network attacks, ensure the authenticity of electronic evidence, and improve the admissibility rate of electronic evidence.

Mpyana Mwamba Merlec et al., (2022):- Electronic portfolios (e-portfolios) are gaining popularity among students and lifelong learners, serving as digital multimedia resumes showcasing their skills and accomplishments. To ensure the integrity of learning achievements, e-portfolios require secure and reliable credential issuance and verification mechanisms. However, current systems often rely on centralized solutions provided by private institutions, creating potential problems with credential authenticity and control.

To address these challenges, we propose a decentralized e-portfolio management scheme based on consortium blockchain technology. Leveraging smart contracts, learners gain full ownership and control over their e-portfolio, while potential employers can verify credentials without relying on third parties. Blockchain acts as an immutable ledger, ensuring tamper-proof data provenance and accountability.

Decentralized identifiers and verifiable credentials authenticate user profiles, while verifiable claims validate e-portfolio credentials. Our prototype, implemented on the Quorum Consortium blockchain network, demonstrates the feasibility, security, and privacy-preserving performance of our solution..

Prakrut Chauhan et.al (2021):- Authenticating and verifying digital documents has become crucial as more documents are now being created, modified, and shared in digital formats. Unlike physical copies, ensuring the legitimacy of digital documents poses a challenge. Hence, there's a pressing need for an efficient method to authenticate and verify them.

A decentralized application designed to address this challenge. The application utilizes a smart contract built on blockchain technology to streamline the authentication and verification process for digital documents. Unlike conventional methods that involve storing entire digital documents, this approach employs cryptographic hash functions to generate unique fingerprints for each input document. These fingerprints are then securely stored on the blockchain network, enabling easy verification of documents in the future.

Organizations can leverage this blockchain-based solution to authenticate the documents they produce and grant verification access to other relevant entities. This innovative approach not only enhances document security but also streamlines the verification process, offering a reliable solution for organizations dealing with digital documentation.

Tharaka Hewa et.al (2021): -One of the revolutionary technological advancements in the modern computer paradigms is blockchain. With the help of blockchain technology and smart contracts, many apps that are generally renowned for being difficult and complex have the good fortune to improve the service. The majority of applications are revolutionised with optimal and effective functionality by the decentralised, autonomous operation and built-in transparency of blockchain-based smart contracts. The important implementations that have already profited from smart contracts are examined in this study. From the standpoint of these applications, we also emphasise the future potential of blockchain-based smart contracts.

Mohammed Shuaib et al. (2020) - At every point, the traditional land register system is vulnerable to different kinds of manipulation, which might have serious consequences. These problems affect not just the finances by requiring a lot of record storage and wasteful usage, but they also raise security risks with regard to the integrity of these documents. Moreover, the inefficiencies within the system lead to protracted verification and updating procedures, which in turn creates avenues for corruption and the escalation of fraudulent operations like double spending, which involves the simultaneous sale of a single plot of land to numerous customers. These kinds of structural defects damage the economy by creating mistrust in the land trade industry and preventing economic expansion in general. Furthermore, these shortcomings impede government efforts to collect taxes and income, which in turn makes it easier for illegal monies to proliferate through covert real estate transactions. But the incorporation of Blockchain technology has the potential to help with these urgent issues.

A robust framework for establishing a secure and dependable land registry system is proposed to mitigate the aforementioned concerns. By leveraging blockchain technology, this system aims to thwart tampering and double spending while facilitating near real-time updates of land records. Notably, the proposed solution boasts cost-effectiveness by minimizing reliance on human resources and enhancing reliability.

Yustus Eko Oktian et al. (2020) - A sophisticated blueprint for ensuring the ongoing integrity of IoT big data management via blockchain technology is outlined across three pivotal phases: data transmission, data storage, and data processing. The initial step involves elucidating the motivations driving each phase and conducting a comprehensive survey of existing blockchain research to serve as foundational elements for our design. Subsequently, our solutions are delineated. To safeguard data during transit, we advocate for decentralized identity management and the establishment of secure channels based on blockchain technology. For data storage, we propose the utilization of a series of signatures in conjunction with blockchain receipts to fortify the integrity of stored IoT data. Finally, we

introduce a blockchain-powered decentralized marketplace and federated learning framework to facilitate collaboration among IoT entities during the data processing phase.

Mehmet Aydar et al. (2019) - The Covid-19 pandemic has prompted individuals and organizations to reassess approaches to identity verification and credential sharing, especially in situations requiring quarantine. This research delves into the shortcomings of conventional identity systems and explores the potential for Blockchain technology to establish more secure, privacy-centric, and remote-accessible identity systems. Accordingly, a Blockchain-based framework for digital identity verification, record attestation, and sharing. We elucidate this framework with specific use cases, emphasizing its capacity to empower individuals with full control over their identity data and the extent of its sharing.

Balaji S et al. (2019) - A Blockchain-based land registry offers numerous advantages over traditional centralized database systems. Instead of relying on locally-maintained real estate records, Blockchain serves as the primary repository for property title information. This secure property ownership recording system, outlined in our paper, mitigates potential failures and attacks in the property registration process by leveraging transparency and cryptographic primitives for authentication. Consequently, it diminishes dependence on trusted third parties, lowers costs, and minimizes fraud and errors in property registration and title transfers. The utilization of blockchain-based cryptocurrencies ensures secure and digital fund transfers from buyer to seller, enhancing the efficiency and security of property title transfers. Moreover, the implementation of smart property cards provides authenticity and unique identification for property ownership titles, thereby reducing disputes related to property ownership.

3. A DIGITAL SOLUTION TO NOTARY ACTIVITIES

An electronic (digital) notary gives an official the ability to carry out the notarizing function electronically. Notaries public have had the capabilities of using technology (e.g., digital signatures and digital notary seals for the validation of certificates) for some time now. The electronic notary affixes the authorized seal and signature to the certified document. This notary publicly manages, creates, stores, and distributes the digital certification using cryptography and a protected public key.

Maintaining an electronic record of the notary duties completed is necessary in the case of the digital notary. More significantly, notary public operations may be remotely completed with the use of digital technology.

One of the most notable advancements in the modernization of notary services is the integration of digital technologies. Many advantages come with digitalization, including the simplification of conventional notary procedures and improvements in effectiveness, security, and accessibility.

Digital notary solutions use technology to enable transactions remotely, doing away with the necessity for in-person presence while preserving the legitimacy and integrity of papers. The use of blockchain technology, cryptography, and electronic signatures are essential for guaranteeing the authenticity and immutability of digital documents. Notaries may handle and preserve documents electronically with security thanks to digital platforms, which minimises paperwork and administrative effort. Authorised parties may easily access cloud-based systems, which facilitates quick document retrieval and improves stakeholder cooperation. Additionally, improved authentication capabilities are provided by digital notary solutions, enabling signatory verification in real-time and documentary security. Sophisticated encryption methods protect private data, guaranteeing privacy laws' observance and secrecy.

Notary operations have undergone a digital revolution that has improved security, streamlined procedures, and increased accessibility. Digital technologies have made it possible to carry out notary

functions online effectively and safely, including document authentication, certification, and verification.

Electronic signatures are a major digital solution used in notary operations. With the use of electronic signatures, parties can sign documents electronically without having to be present in person or use paper-based signatures. Modern encryption methods make electronic signatures legally enforceable in many countries by guaranteeing their integrity and validity.Blockchain technology is a crucial component of digital notary systems. Blockchain technology offers an immutable, decentralised, and tamper-proof ledger for recording notary operations. This lowers the possibility of fraud and assures the traceability and integrity of papers and transactions.

4. CONCLUSION

A blockchain-based digital notary system offers a robust solution for timestamping and verifying digital documents, providing reliability and tamper-proof features. By leveraging the distributed and immutable nature of blockchain technology, such a system ensures that timestamps are secure and cannot be altered retroactively. Furthermore, there is no single point of failure or control, the decentralised structure of blockchain networks improves confidence and transparency in this verification processes. All things considered, putting in place a blockchain-based digital notary system may greatly improve the legitimacy and integrity of digital writings making it a useful tool for a variety of sectors and applications.

REFERENCES

1. Jiahao Zhao, Yushu Zhang , Jiajia Jiang , Zhongyun Hua , Yong Xiang. “A secure dynamic cross-chain decentralized data consistency verification model”, Volume 36, Issue 1, January 2024, 101897.
2. Monther Aldwairi, Mohamad Badra, and Rouba Borghol "DocCert: Nostrification, Document Verification and Authenticity Blockchain Solution" 2023.
3. Lei Shang; Xiaoyan Yang; Xuanrong Chen. "A Blockchain-based Electronic Data Forensics System DesignandImplementation." *10.1109/DSPP58763.2023.10405059* (2023).
4. Mpyana Mwamba Merlec,Md. Mainul Islam ,Youn Kyu Lee and Hoh Peter “A Consortium Blockchain-Based Secure and Trusted Electronic Portfolio Management Scheme” Volume 22, Issue 3, 8 February 2022.
5. Prakrut Chauhan, Jai Prakash Verma, Swati Jain & Rohit Rai “Blockchain Based Framework for Document Authentication and Management of Daily Business Records” pp 497–517 2021.
6. Tharaka Hewa, Mika Ylianttila, Madhusanka Liyanage “Blockchain based Smart Contracts: Applications, Opportunities and Challenges” October 30,2021.
7. Mohammed Shuaib, Salwani Mohd Daud, Shadab Alam , Wazir Zada Khan “Blockchain-based framework for secure and reliable land registry system” Vol. 18, No. 5, October 2020, pp. 2560~2571.
8. Yustus Eko Oktian , Sang-Gon Lee and Byung-Gook Lee “Blockchain-Based Continued Integrity Service for IoT Big Data Management: A Comprehensive Design” 3 September 2020.
9. Mehmet Aydar · Serkan Ayvaz · Salih Cemil C¸ etin “Towards a Blockchain based digital identity verification, record attestation and record sharing system” 23 Jun 2019.
10. Balaji S “BlockChain based Secure Smart Property Registration Management System and Smart Property Cards” Volume 7 Issue VI, June 2019, ISSN: 2321-9653

11. S. Nakamoto, Bitcoin: A Peer-to-peer Electronic Cash System, 2009. URL: http://www.bitcoin.org/bitcoin.pdf.
12. V. Buterin, et al., A Next-generation Smart Contract and Decentralized Application Platform, white paper 3 (2014) 37.
13. S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin, F.-Y. Wang, An Overview of Smart Contract: Architecture, Applications, and Future Trends, in: 2018 IEEE Intelligent Vehicles Symposium (IV), IEEE, 2018, pp. 108–113.
14. A. Wright, P. De Filippi, Decentralized Blockchain Technology and the Rise of Lex Cryptographia, Available at SSRN 2580664 (2015).
15. C. Udokwu, A. Kormiltsyn, K. Thangalimodzi, A. Norta, An Exploration of Blockchain Enabled Smart-contracts Application in the Enterprise, Technical Report, Technical Report, DOI: 10.13140/RG. 2.2. 36464.97287, Tech. Rep, 2018.
16. P. L. Seijas, S. J. Thompson, D. McAdams, Scripting smart contracts for distributed ledger technology., IACR Cryptology ePrint Archive 2016 (2016) 1156.
17. S. Aggarwal, R. Chaudhary, G. S. Aujla, N. Kumar, K.-K. R. Choo, A. Y. Zomaya, Blockchain for Smart Communities: Applications, Challenges and Opportunities, Journal of Network and Computer Applications (2019).
18. K. Wust, A. Gervais, Do You Need a Blockchain?, in: 2018 Crypto ¨ Valley Conference on Blockchain Technology (CVCBT), IEEE, 2018, pp. 45–54.
19. C. D. Clack, V. A. Bakshi, L. Braine, Smart Contract Templates: Essential Requirements and Design Options, arXiv preprint arXiv:1612.04496 (2016).
20. L. Chen, L. Xu, N. Shah, Z. Gao, Y. Lu, W. Shi, Decentralized Execution of Smart Contracts: Agent Model Perspective and its Implications, in: International Conference on Financial Cryptography and Data Security, Springer, 2017, pp. 468–477.
21. J. Sousa, A. Bessani, M. Vukolic, A Byzantine Fault-tolerant Ordering Service for the Hyperledger Fabric Blockchain Platform, in: 2018 48th annual IEEE/IFIP international conference on dependable systems and networks (DSN), IEEE, 2018, pp. 51–58.
22. X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, P. Rimba, A taxonomy of Blockchain-based Systems for Architecture Design, in: 2017 IEEE International Conference on Software Architecture (ICSA), IEEE, 2017, pp. 243–252.
23. B. Marino, A. Juels, Setting Standards for Altering and Undoing Smart Contracts, in: International Symposium on Rules and Rule Markup Languages for the Semantic Web, Springer, 2016, pp. 151–166.
24. A. Norta, Designing a Smart-contract Application Layer for Transacting Decentralized Autonomous Organizations, in: International Conference on Advances in Computing and Data Sciences, Springer, 2016, pp. 595– 604.
25. L. Luu, Y. Velner, J. Teutsch, P. Saxena, Smartpool: Practical Decentralized Pooled Mining, in: 26th {USENIX} Security Symposium ({USENIX} Security 17), 2017, pp. 1409–1426.
26. P. Dai, N. Mahi, J. Earls, A. Norta, Smart-contract Value-transfer Protocols on a Distributed Mobile Application Platform, URL: https://qtum. org/uploads/files/cf6d69348ca50dd985b60425ccf282f3. pdf (2017) 10.
27. D. Macrinici, C. Cartofeanu, S. Gao, Smart Contract Applications within Blockchain Technology: A Systematic Mapping Study, Telematics and Informatics (2018).

28. Z. Zheng, S. Xie, H.-N. Dai, X. Chen, H. Wang, Blockchain Challenges and Opportunities: A Survey, International Journal of Web and Grid Services 14 (2018) 352–375.
29. P. He, G. Yu, Y. Zhang, Y. Bao, Survey on Blockchain Technology and its Application Prospect, Computer Science 44 (2017) 1–7.
30. L. S. Sankar, M. Sindhu, M. Sethumadhavan, Survey of Consensus Protocols on Blockchain Applications, in: 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE, 2017, pp. 1–5.
31. A. Singh, K. Click, R. M. Parizi, Q. Zhang, A. Dehghantanha, K.-K. R. Choo, Sidechain Technologies in Blockchain Networks: An Examination and State-of-the-art Review, Journal of Network and Computer Applications (2019) 102471.
32. M. Bartoletti, L. Pompianu, An empirical analysis of smart contracts: platforms, applications, and design patterns, in: International conference on financial cryptography and data security, Springer, 2017, pp. 494– 509.
33. J. Sengupta, S. Ruj, S. D. Bit, A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT, Journal of Network and Computer Applications (2019) 102481.
34. Q. Feng, D. He, S. Zeadally, M. K. Khan, N. Kumar, A Survey on Privacy Protection in Blockchain System, Journal of Network and Computer Applications 126 (2019) 45–58