INTERNATIONAL JOURNAL OF INNOVATIVE STUDIES
A MONTHLY, INDEXED, REFEREED AND PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
Vol. 5. Issue. 1. 2024 (May)

RESEARCH ARTICLE

ISSN: ISSN: 3027-2173

ACHIEVING DATA INTEGRITY IN DIGITAL LIBRARIES THROUGH IMPLEMENTATION OF BLOCKCHAIN TECHNOLOGY

Patience Uloaku IKEGWUIRO
Research and Technical Services Department, National Water Resources Institute, P.M.B. 2309, Mando, Kaduna, Kaduna State
Email: bankike2@gmail.com

Rose Toyin OGALUE
Quality Assurance/ICT Department , National Teachers Institute, Kaduna State
Email: ogaluerosetoyin@gmail.com

Article Information

Received: 09th April, 2024
Accepted: 11th May, 2024
Published: 28th May, 2024

Keywords: Blockchain, Data Integrity and Digital Libraries

PUBLISHER: Empirical Studies and Communication–(A Research Center)
Website: www.cescd.com.ng

Abstract

Digital libraries are essential for the preservation and distribution of extensive volumes of information across many disciplines. Maintaining the accuracy and genuineness of the data housed in these repositories continues to be a major obstacle. Conventional centralized systems are exposed to vulnerabilities such as having a single point of failure and being prone to data tampering. In order to tackle these challenges, this article suggests using blockchain technology to improve the reliability of data in digital libraries. Blockchain, the foundational technology underpinning cryptocurrencies such as Bitcoin, provides a decentralized and unchangeable ledger that documents transactions across a network of nodes. Through the integration of blockchain technology in digital libraries, every individual data element may be securely connected and assigned a timestamp, resulting in a visible and impervious record of its chronological sequence. This guarantees that once data is inputted into the system, it cannot be modified or erased without agreement from the members in the network. This study examines the theoretical foundation and practical use of blockchain technology in digital libraries with the goal of ensuring data integrity. The text explores the fundamental elements of blockchain technology, including as blocks, consensus processes, and smart contracts, and how they may be customized to meet the special needs of digital library systems.

Introduction

Data security has emerged as a prominent concern on a worldwide scale (Omoyiola, 2018). There are several data hazards present in all areas. Security risks manifest as vulnerabilities, hackers, data breaches, insider threats, and human employee mistakes. To prevent harm, these risks must be managed (Omoyiola, 2019). The hazards may be difficult to prevent, but it is possible to reduce their impact (Omoyiola, 2018b). Blockchain has emerged as a viable method for addressing the issue of data trust. By using cryptography and encryption techniques, it reduces the likelihood of data tampering and enhances the protection of data confidentiality (Zheng et al., 2018). Hence, it became imperative to devise a method for verifying data integrity while conserving bandwidth and computational resources. Lately, there has been a growing focus on examining distant data via remote data auditing in order to verify the integrity and accuracy of data stored in remote locations. Data integrity, for the users of the data system, refers to the state of being complete, unimpaired, unmodified, and free from any kind of harm. Data integrity refers to the state of data that remains unaltered by a hacker or an unauthorized invader (Akeson, 1989). Data integrity refers to the state of data being unaltered and unaffected by unauthorized individuals, such as hackers or intruders (Akeson, 1989). It also refers to data that remains intact and unharmed despite any deficiencies or system failures. Data corruption and breaches in system data may occur due to human mistake, data manipulation, system breakdown, or environmental disaster. Organizations and system users that rely on the accuracy and reliability of data should adopt strategies and approaches to ensure data integrity (Akeson, 1989).

Digital libraries have become an essential component of the information environment, offering a massive reservoir of knowledge and information that can be accessed by people across the globe. These libraries include a wide range of digital resources, such as papers, photos, videos, and other types of media. Preserving the accuracy and reliability of data in digital libraries is a top priority for librarians, archivists, and information workers. In order to preserve the value and usefulness of digital assets, it is crucial to ensure their trustworthiness and authenticity.

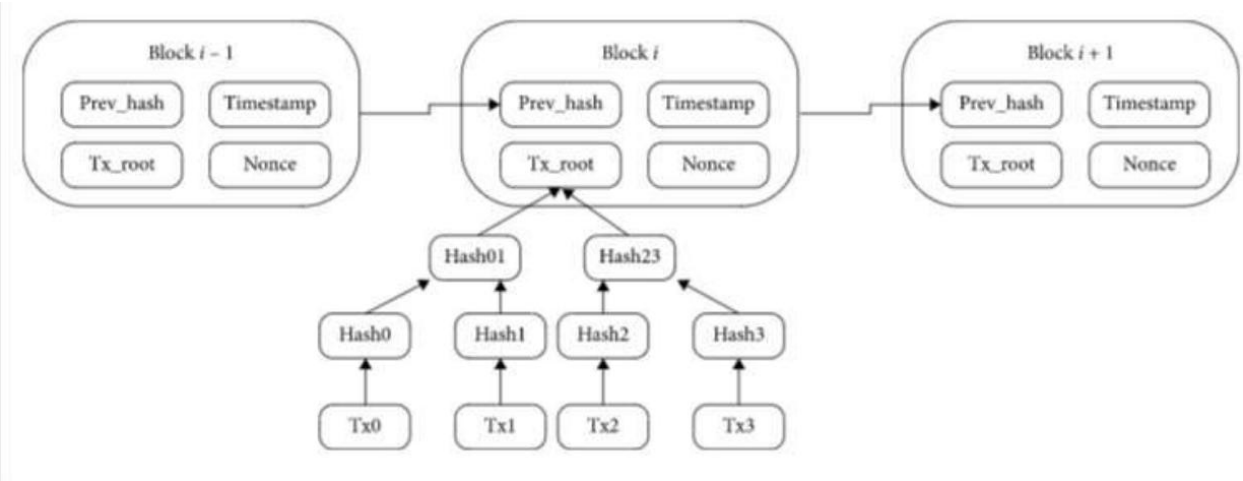
Conventional approaches to guaranteeing the accuracy and reliability of data mostly depend on centralized systems that are built on trust. Nevertheless, these systems are not infallible and are prone to several vulnerabilities, such as data manipulation and illegal intrusion. Blockchain technology, first recognized for its association with cryptocurrencies such as Bitcoin, provides a decentralized and unchangeable ledger for documenting transactions. The potential uses of blockchain technology go beyond financial transactions and may be used to tackle the issues of data integrity in digital libraries.

Although the digital revolution has brought many benefits to libraries and information management, concerns over the reliability and credibility of data still remain. Libraries face the risk of illegal alterations, removals, or damage to their digital holdings. Furthermore, consumers often depend on the reliability of the library administration, which may not be consistently assured. The topic at hand may be succinctly stated as: how can blockchain technology be used to improve the reliability and confidence in digital libraries by tackling concerns about data manipulation, unlawful entry, and the centralized structure of conventional data management systems?

Overview of Blockchain Technology

The word "blockchain" refers to the process of linking digital blocks that contain data. Every data block is designed to possess an intricate cryptographic link to the preceding block in the chain. The creation of the data chain enables this kind of communication. Nofer et al. (2017) argue that if a block is modified, it is necessary to update all subsequent blocks in order to maintain the integrity of the chain. This is due to the need that every block in the chain must possess a high level of security in order for the whole system to function effectively. If you fail to do so, all blocks following the one being changed will be invalidated.

Figure 1.: Blockchain Architecture



Blockchain is a decentralized database that stores records or a public ledger of all electronic transactions or digital events that are completed and shared among members. The verification of transactions in the public ledger is achieved by the consensus of a majority of the participants in the system. Blockchain technology ensures that intruders are unable to delete any recorded information. The blockchain has the capability to be used in several domains such as cash, smart contracts, record keeping, ID systems, cloud storage, and numerous more application sectors. In 2018, Lieutenant suggested a blockchain architecture consisting of four components: Data Owners Application (DOA), Data Consumer Applications (DCAs), Cloud Storage Service, and Blockchain. The purpose of the blockchain-based

architecture for Data Integrity Service is to enhance the dependability of data integrity verification for Data Owners and Data Consumers, eliminating the need for a Third Party Auditor (TPA).

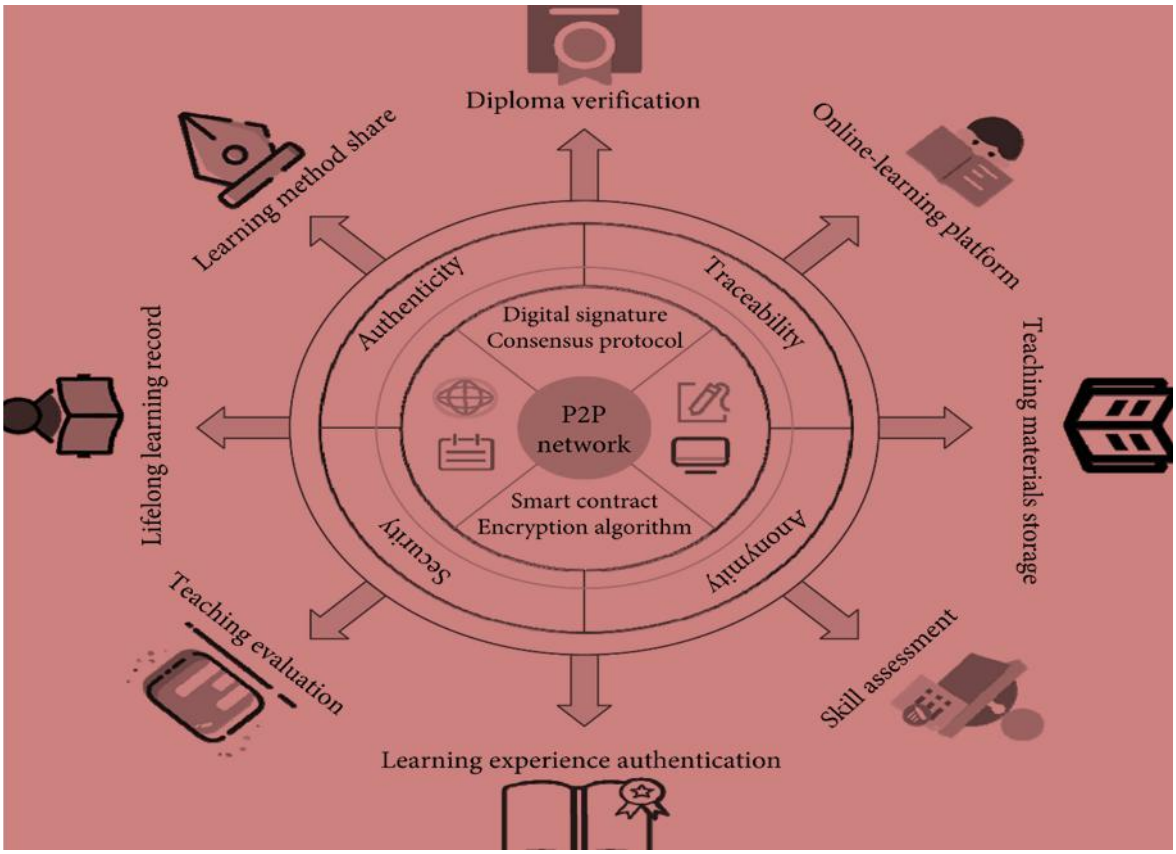


Fig. 2: Blockchain Functionality

Blockchain, a decentralized system for recording and organizing digital information, provides a novel approach to data management and aggregation. According to Gilder (2018), several specialists in digital technology see this as the start of a new megatrend. Nevertheless, the issue of the extent to which technology may be beneficial in the classroom remains unresolved. There is no denying the extensive impact it has. It may be used in many settings, such as educational administration. The academic records of a student, which consist of their marks, papers, and certificates, are saved on a decentralized ledger. It provides protection for students when they showcase their knowledge in exams and other activities, and it simplifies the process of verifying their identification (STM Future Technology Institute, 2022).

Security Analysis of Blockchain Technology

Blockchain is a decentralized system of recording information that was first created in 2008 for the Bitcoin platform. It has the ability to address the issue of trust in several scenarios. Organizations in the financial sector are now investigating the potential success of integrating blockchain technology into their existing software.

This integration aims to fulfill the need for a more transparent and unchangeable audit log (Khan, Lewis, Rutland, Wan, Rutter, & Thompson, 2017). Blockchain applications in several sectors, including healthcare, have lately gained considerable interest. Blockchain has been suggested as a potential remedy for overseeing patients and granting identities, authorization for healthcare data, and maintaining participant consent. As to Zheng et al. (2018), the use of developing cryptographic technologies, like blockchain, has the potential to decrease the likelihood of data tampering and enhance trust in data. Blockchain is a fundamental notion of Bitcoin, functioning as both a decentralized database and the underlying technology of Bitcoin (Crosby, 2016). A blockchain is a sequential collection of data blocks that are created using cryptographic techniques, as seen in Figure 2. Each block in the Bitcoin network includes information about a transaction and is used to verify the authenticity of the data and create the following block. Blockchain is a specific kind of data structure that links data blocks in a sequential manner based on time and is secured using cryptography, forming a distributed ledger that is resistant to tampering or forgery. Blockchain technology utilizes blockchain data structures to authenticate and store data in a comprehensive manner. The system employs distributed node consensus techniques for data generation and updates, utilizes encryption for secure data transfer and access, and employs intelligent contracts consisting of automated script code for data programming and manipulation. Blockchain has the attributes of decentralization, immutability, traceability, collaborative maintenance, openness, and transparency. The qualities of blockchain guarantee integrity and openness, establishing the basis for fostering trust. The blockchain's extensive range of applications stems from its ability to address information asymmetry and facilitate collaborative trust and coordinated actions among different entities. Conducting a security study of blockchain technology is essential for comprehending the advantages and disadvantages of this groundbreaking decentralized record-keeping system. Blockchain has several security functionalities, although it also encounters certain security obstacles. Presented below is an exhaustive security examination of blockchain technology:

Security Features of Blockchain Technology

Decentralization:

Strength: Blockchain operates on a decentralized network of nodes, making it resistant to single points of failure and reducing the risk of centralized control and data manipulation.

Cryptography:

Strength: Strong cryptographic techniques are used to secure data and transactions, making it difficult for unauthorized parties to tamper with or read sensitive information.

Immutable Ledger:

Strength: Once data is added to the blockchain, it is nearly impossible to alter or delete, ensuring data integrity.

Consensus Mechanisms:

Strength: Various consensus mechanisms (e.g., Proof of Work, Proof of Stake) ensure that network participants agree on the validity of transactions, mitigating the risk of fraudulent activities.

Transparency:

Strength: Transactions on the blockchain are transparent and can be audited by anyone, promoting accountability.

Smart Contracts:

Strength: Self-executing smart contracts enable automated, tamper-resistant execution of predefined agreements without intermediaries.

Permissioned Blockchains:

Strength: Private and consortium blockchains provide greater control and privacy for organizations, while still leveraging blockchain's security benefits.

Security Challenges and Concerns:

51% Attacks:

Concern: In Proof of Work blockchains, a malicious entity controlling over 50% of the network's computational power could potentially manipulate the blockchain.

Consensus Vulnerabilities:

Concern: Consensus algorithms are not immune to attacks. For example, Proof of Stake blockchains can be vulnerable to the "Nothing at Stake" problem.

Smart Contract Vulnerabilities:

Concern: Flaws in smart contract code can lead to vulnerabilities, allowing attackers to exploit these contracts and steal funds.

Privacy Concerns:

Concern: While blockchain transactions are pseudonymous, additional data can be linked to individuals or entities, potentially compromising privacy.

Scalability:

Concern: As the blockchain grows, maintaining security and decentralization while achieving scalability is a challenge.

Regulatory and Legal Challenges:

Concern: Adhering to local and international regulations while maintaining blockchain's trustless and borderless nature can be complex.

Interoperability:

Concern: Interoperability between different blockchains and legacy systems poses challenges in data sharing and security.

Network Upgrades and Forks:

Concern: Upgrading or forking a blockchain can introduce security risks, as not all participants may agree on the changes.

Loss of Private Keys:

Concern: If a private key is lost or stolen, the associated assets can become irretrievable.

Social Engineering and Phishing Attacks:

Concern: Attack vectors targeting individual users and organizations can lead to loss of funds or data breaches.

Mitigation Strategies:

Diverse Consensus Mechanisms: Exploring different consensus mechanisms can reduce the risk of 51% attacks and other vulnerabilities.

Smart Contract Auditing: Thoroughly auditing smart contract code before deployment can help prevent vulnerabilities.

Privacy Solutions: Implementing privacy-enhancing technologies like zero-knowledge proofs can address privacy concerns.

Scalability Solutions: Implementing layer-2 solutions like the Lightning Network (for Bitcoin) and sharding (for Ethereum) can improve scalability.

Regulatory Compliance: Collaborating with regulators and implementing Know Your Customer (KYC) and Anti-Money Laundering (AML) measures can ensure compliance.

Secure Key Management: Proper key management practices, including hardware wallets and multi signature wallets, can mitigate the risk of key loss or theft.

Security Training: Educating users and organizations about best security practices can help prevent social engineering and phishing attacks.

Regulatory Compliance Challenges

Businesses have substantial obstacles in complying with data protection standards such as CCPA (California Consumer Privacy Act), GDPR (General Data Protection Regulation), or PCI DSS (Payment Card Industry Data Security Standard) [Treiblmaier, et al 2021]. These laws enforce stringent guidelines on the handling and safeguarding of sensitive data, including customer information [Treiblmaier, et al 2021]. An important obstacle is in the intricacy of these standards, which often include precise and elaborate instructions that organizations are obligated to adhere to. Achieving compliance and efficiency in e-commerce operations may be challenging due to the need for significant resources, time, and knowledge to execute the required modifications in processes, systems, and regulations [Treiblmaier, et al 2021]. Effectively managing compliance requirements while ensuring seamless e-commerce operations is a substantial challenge. Companies must allocate resources towards implementing strong data security measures, providing comprehensive staff training, establishing a secure technical infrastructure, and conducting frequent audits. These actions are necessary to comply with rules and maintain ongoing e-commerce operations.

Privacy Concerns:

Concern: Although blockchain transactions provide pseudonymity, it is possible to associate extra data with persons or organizations, which might possibly jeopardize privacy.

Scalability:

Concern: As the blockchain grows, maintaining security and decentralization while achieving scalability is a challenge.

Regulatory and Legal Challenges:

Concern: Ensuring compliance with both local and international legislation while preserving the trustless and borderless characteristics of blockchain technology may be a challenging task.

Interoperability:

Concern: Data sharing and security are challenging when it comes to interoperability across various blockchains and traditional systems.

Network Upgrades and Forks:

Concern: Implementing upgrades or creating a separate version of a blockchain might potentially pose security vulnerabilities, since there may be disagreements among participants on the modifications.

Loss of Private Keys:

Concern: If a private key is misplaced or unlawfully obtained, the corresponding assets may become permanently unattainable.

Social Engineering and Phishing Attacks:

Concern: Individual and businesses might suffer financial losses or data breaches as a result of targeted attack vectors.

Mitigation Strategies:

Diverse Consensus Mechanisms: By examining various consensus processes, the potential for 51% attacks and other weaknesses may be mitigated.

Smart Contract Auditing: Conducting a comprehensive audit of smart contract code prior to deployment may effectively mitigate risks.

Privacy Solutions: Privacy problems may be effectively addressed by using privacy-enhancing technology such as zero-knowledge proofs.

Scalability Solutions: Scalability may be enhanced by using layer-2 technologies such as the Lightning Network for Bitcoin and sharding for Ethereum.

Regulatory Compliance: Ensuring compliance may be achieved by collaborating with authorities and adopting procedures such as Know Your Customer (KYC) and Anti-Money Laundering (AML).

Secure Key Management: Implementing effective key management techniques, such as utilizing hardware wallets and multi signature wallets, helps reduce the likelihood of losing or having keys stolen.

Security Training: Disseminating knowledge to consumers and businesses about optimal security protocols may effectively mitigate the risk of social engineering and phishing assaults.

Applications of Blockchain Technology

Blockchain is a decentralized system of recording information that was first created in 2008 for the Bitcoin platform (Crosby, Pattanayak, & Verma, 2016). Blockchain is a distributed ledger that use cryptography to ensure that data blocks are combined in a sequential manner according to the time sequence. It is a tamper-proof data

structure. Financial institutions are already investigating the potential success of integrating blockchain technology into their current software to meet the need for a more transparent and unchangeable audit log (Khan et al., 2017). Blockchain applications in several sectors, such as healthcare, have lately garnered considerable interest. Blockchain has been suggested as a potential remedy for overseeing patients and granting identities, authorization to healthcare data, and controlling participant consent. The emergence of blockchain technology provides a reliable assurance of trust. The system employs a consensus technique to guarantee data consistency across nodes and an encryption mechanism to maintain data security (Xie et al., 2021). Blockchain is a cryptographic distributed ledger that joins data blocks in a chronological sequence, ensuring that it is tamper-proof and cannot be forged. Blockchain participants uphold the node information of a blockchain by providing open and transparent data on the network. The released information is securely stored and cannot be altered. The blockchain's open verification and tamper-proof capabilities serve as a reliable intermediary to answer consumers' worries in the cloud computing environment. By incorporating the blockchain into a cloud computing environment, users may ensure data security since all outcomes can be authenticated and stored on the blockchain, accessible to all users (Crosby et al., 2016). In essence, blockchain technology utilizes blockchain data structures to authenticate and store data. IT use distributed node consensus techniques to produce and update data, using encryption to provide secure data transfer and access. Additionally, it utilizes smart contracts, which consist of automated script code, to program and change the data. Blockchain has distinct attributes such as decentralization, immutability, traceability, collaborative maintenance, openness, and transparency.

Analysis of Existing Measures for Assurance of Data Integrity

There are several established methods for guaranteeing data integrity, such as generating checksum values and comparing them to reference values. These methods include key and keyless hashing, as well as cryptographic techniques like electronic signatures (Dichenko & Finko, 2018). One drawback of these systems is their inability to guarantee integrity without the inclusion of an extra data recovery mechanism. Additional approaches to guarantee data integrity include using several forms of reservation such as hardware or software implementation of RAID technology (Redundant Array of Independent Disks) (RAID arrays), duplication techniques, and redundant coding methods. An inherent drawback of these approaches is their substantial redundancy (Dichenko & Finko, 2018). Khan et al. (2017) created Trial Chain, a blockchain-powered platform, to enhance the visibility and analysis of data quantity in major biomedical research projects. This platform ensures the integrity of the data. According to Whyte (2018), a dependable data gathering process is crucial for the effective functioning of an analytic system, since the correctness of the data is directly influenced by the methods used for data collection. The study used the Multi Chain platform to establish a private blockchain and seamlessly connected it with a data science platform deployed inside a

prominent research institution. Ensuring the accuracy and documentation of analytic stages is crucial for effectively using the findings to provide high-quality clinical care.

Data integrity is a crucial topic in several domains, such as digital libraries, data management, and cybersecurity. Various established processes and approaches have been created to guarantee and authenticate the integrity of data. Here is an examination of many of these measures:

Hash Functions:

Description: Hash functions are computational procedures that convert data into a consistent and predetermined sequence of characters, usually represented as a hexadecimal numeral. Their purpose is to generate a distinct hash value for every distinct collection of data.

Analysis: Hash functions are extensively used for the purpose of verifying the integrity of data. By doing a comparison between the hash value of the original data and the hash value of the received data, any inconsistencies or modifications may be identified. Widely used hash functions are MD5, SHA-1, and SHA-256.

Strengths: Fast computation, efficient for large datasets, easy to implement.

Weaknesses: Prone to collision attacks, which occur when two distinct inputs generate the same hash value. Therefore, not recommended for standalone authentication purposes.

Digital Signatures:

Description: Asymmetric cryptography is used by digital signatures to provide authenticity and data integrity. A private key is used for the purpose of digitally signing data, whereas a matching public key is employed to authenticate and validate the signature.

Analysis: Digital signatures guarantee the integrity and validity of data. They can verify that the data has not been modified and was signed by the anticipated sender.

Strengths: Robust security measures, ensures the inability to deny involvement, extensively embraced for safe communication. (Mishra, Alzoubi, Gill, & Anwar, 2022).

Weaknesses: The process may incur significant computational costs and necessitates the involvement of a reliable certificate authority, as well as careful management of cryptographic keys.

Cryptographic Hash Chains:

Description: Cryptographic hash chains consist of a series of hash values, where each value is derived from the preceding one via computation. They are used to generate an indubitable record of alterations in data (Shiksha Online, 2023).

Analysis: Cryptographic hash chains are a reliable method for monitoring changes to data over a period of time, offering a means to identify any unauthorized modifications. They are often used in the field of blockchain technology. (Sungbeen Kim and Dohoon Kim, 2024)

Strengths: Offers a comprehensive record of data modifications, designed to detect any tampering attempts and highly resistant to any revisions.

Weaknesses: Difficult to handle, requiring a significant amount of resources for lengthy chains.

Models to Ensure Data Integrity with Blockchain

Safeguarding the authenticity and security of data storage and transmission is a significant obstacle. Therefore, data encryption requires the use of cryptographic algorithms that need extra time. The article introduces blockchain technology as a means to ensure the integrity of data. Vainshtein and Gudes (2021) introduced a new approach that utilizes a Proof-of-Work (PoW) based Blockchain to guarantee data integrity in cloud database management systems. This technique aims to address the challenges associated with utilizing cloud platforms for data storage and database hosting. The model used an interaction mechanism using the cloud platform and a Proof-of-Work (PoW) based Blockchain. Due to the lack of a practical method for clients to verify the integrity of data stored in the cloud database, this strategy utilizes a Distributed Hash Table and lightweight software agents to monitor changes made to storage nodes in the cloud database. When the agents engage, they publish the data update activities as Blockchain log/audit transactions into the Blockchain network. These transactions are safeguarded by the Blockchain network via immutability and cryptographic measures. The suggested technique allows the Cloud Provider to efficiently handle metadata in order to promptly identify intentional or unintentional transaction corruptions and to restore transactions in the event of any data corruption incidents (Wu et al., 2019). Ensuring the accuracy and security of large-scale data stored in cloud storage is now a prominent area of focus. The conventional approach to ensuring data integrity involves using encryption methods to safeguard data stored in the cloud, with the assistance of trustworthy Third-Party Auditors (TPAs). However, this method is being replaced by the use of Blockchain technology. Blockchain-based data integrity methods effectively circumvent the issue of trust associated with TPAs. In their study, Wang and Zhang (2019) tackled the challenges of TPAs by introducing a Data Integrity Scheme (BB-DIS) that utilizes Blockchain and Bilinear mapping. This scheme is specifically designed to ensure the integrity of large-scale IoT data.

Conclusion

This investigation of the capacity of blockchain to guarantee data integrity in digital libraries reveals that blockchain technology presents a hopeful resolution to the enduring obstacles of data integrity and trust in the field of digital libraries. Digital libraries, which store significant knowledge and information, have challenges related to data tampering, unlawful access, and dependence on centralized data management systems. Blockchain, due to its decentralized nature, inability to be altered, and capacity to offer clear visibility, has the potential to create a revolutionary structure for protecting the authenticity of digital assets and strengthening confidence.

By doing a thorough examination of current methods and models, it is evident that blockchain technology offers a distinct set of security characteristics that make it a compelling option for digital libraries. It utilizes cryptographic hashing, decentralization, and consensus techniques to guarantee the integrity and reliability of data. This strategy has the potential to radically transform the manner in which digital assets are handled and safeguarded within the realm of libraries. Nevertheless, it is crucial to recognize that the effective incorporation of blockchain technology in digital libraries presents some difficulties and factors to be taken into account. These concerns include scalability, energy consumption (particularly in consensus processes like as Proof of Work), adherence to regulations, and the need for strong key management procedures. Furthermore, it is important to note that blockchain technology cannot be universally used and must be customized to suit the unique requirements and limitations of each digital libraries.

Ultimately, the use of blockchain technology to guarantee the accuracy and reliability of data in digital libraries is a promising avenue that warrants additional investigation and study. Although it is not a cure-all, the distinct array of security characteristics it has may greatly aid in resolving the pressing issues of data integrity and trust in digital libraries. As technology advances and evolves, it has the potential to completely transform the way digital assets are handled, verified, and protected in the digital era. This will eventually improve the quality and dependability of digital libraries for consumers worldwide.

Implication of Findings

The application of blockchain in digital libraries offers several compelling benefits:

Data Immutability: Blockchain ensures that once data is recorded, it becomes practically immutable, rendering unauthorized changes and tampering nearly impossible.

Trust and Transparency: The transparency of blockchain technology builds trust among users as they can independently verify the integrity of data without relying on a centralized authority.

Security: The cryptographic methods used in blockchain ensure the secrecy and integrity of data, enhancing the overall security stance of digital libraries.

Decentralization: Blockchain reduces the likelihood of data breaches and unauthorized access by removing vulnerable points and central control.

Smart Contracts: Smart contracts enable the automation of data validation and management procedures, therefore minimizing human mistakes and guaranteeing the integrity of data.

Timestamping and Audit Trails: The timestamping features of blockchain ensure the creation or modification time of data is permanently recorded, enabling accountability and monitoring of past data.

References

Akeson, J. K. (1989). Assuring system data integrity-An overview. 1989 IEEE Global Telecommunications Conference and Exhibition 'Communications Technology for the 1990s and Beyond', (1), 217-22. http://doi.org/ 10.1109/GLOCOM.1989.63970.

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2(6-10), 71. https://j2-capital.com/wpcontent/uploads/2017/11/AIR-2016-Blockchain.pdf

Department of Computer Science, Kyonggi University, Suwon-si 16227, Republic of Korea; beensk@kyonggi.ac.kr * Correspondence: karmy01@kyonggi.ac.kr

Gilder, G. F. (2018). *Life after Google: The fall of big data and the rise of the blockchain economy*. Washington, DC: Regnery Gateway.

Khan, C., Lewis, A., Rutland, E., Wan, C., Rutter, K., & Thompson, C.(2017). A DistributedLedger Consortium Model for Collaborative Innovation. IEEE Computer. 50 (9), 29-37. http://doi: 10.1109/MC.2017.3571057

Kim, Sungbeen, and Dohoon Kim. 2024. "Data-Tracking in Blockchain Utilizing Hash Chain: A Study of Structured and Adaptive Process" *Symmetry* 16, no. 1: 62. https://doi.org/10.3390/sym16010062

Mishra, A.; Alzoubi, Y.I.; Gill, A.Q.; Anwar, M.J. Cybersecurity Enterprises Policies: A Comparative Study. Sensors 2022, 22, 538. https://doi.org/10.3390/s22020538

Omoyiola, B. O. (2018a). Overview of biometric and facial recognition techniques. IOSR Journal of Computer Engineering (IOSRJCE). 20(4), 1-5.doi: 10.9790/0661-2004010105.

Omoyiola, B. O. (2018b). The hard reality of information security. IOSR Journal of Computer Engineering (IOSR-JCE). 21(6), 16-18.doi:10.9790/0661-2106011618.

The legality of ethical hacking. IOSR Journal of Computer Engineering (IOSR-JCE). 20(1), 61-63.doi:10.9790/0661-2001016163. Omoyiola, B. O. (2019).

Vainshtein, Y., & Gudes, E. (2021). Use of Blockchain for Ensuring Data Integrity in Cloud Databases. In: Dolev S., Margalit O., Pinkas B., Schwarzmann A. (eds) Cyber Security Cryptography and Machine Learning. Lecture Notes in Computer Science, 12716. https://doi.org/10.1007/978-3-030-78086-9_25

Wang, H., & Zhang, J. (2019). Blockchain-Based Data Integrity Verification for Large-Scale IoT Data. IEEE Access. http/:doi:10.1109/ACCESS.2019.2952635Corpus.

Whyte, S. T. (2018). Cyber Forensic and Data Collection Challenges in Nigeria. Global Journal of Computer Science and Technology: G Interdisciplinary, 18(3).

Wu., X, Shi, J., Gao, F., Bao,L., Wang, W., and Li, J. (2019). A blockchain Internet of Things Data Integrity Detection Model. International Conference on Advanced Information Science and System. https://doi.org/10.1145/3373477.3373498.

Xie, G., Liu, Y., Xin, G., & Yang, Q. (2021). Blockchain-Based Cloud Data Integrity Verification Scheme with High Efficiency. Security and Communication Networks. https://doi.org/10.1155/2021/9921209

Zheng, Z., Xie, S., Dai, H., Chen, X., Wang H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services (IJWGS), 14 (4), 352-375. http://doi.org/10.1504/IJWGS.2018.10016848

Zheng, Z., Xie, S., Dai, H., Chen, X., Wang H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services (IJWGS), 14 (4), 352-375. http://doi.org/10.1504/IJWGS.2018.10016848