The Eastasouth Journal of Information System and Computer Science
Vol. 1, No. 02, December, pp. 241-250

Blockchain-Integrated System Architecture for Secure and Transparent Data Transactions

Wajihi Ali[1], Md. Kamal Khan[2], Walid Nguia[3], Okouma Nguia[4]
[1,3] Institute of Educational and Management Technologies, the Open University of Tanzania, Kinondoni, Tanzania
[2,4] Faculty of Sciences, Masuku University of Science and Technology, Franceville, Gabon

Article Info

Article history:

Received Dec, 2023
Revised Dec, 2023
Accepted Dec, 2023

Keywords:

Blockchain-Integrated;
Architecture;
Data Integrity and Transparency;
Distributed Ledger Technology;
Secure Data Transactions;
Smart Contracts

ABSTRACT

The growing demand for secure, transparent, and efficient data transaction systems has highlighted the limitations of traditional centralized architectures, particularly in terms of data integrity, trust, and vulnerability to cyber threats. This study proposes a blockchain-integrated system architecture designed to enhance the security and transparency of data transactions. The proposed framework combines layered system design with decentralized blockchain technology, incorporating user, application, blockchain, off-chain storage, and security layers to ensure robust data handling and verification. The architecture leverages cryptographic techniques such as hashing, encryption, and digital signatures to ensure data confidentiality, integrity, and authentication. Additionally, the use of off-chain storage mechanisms addresses scalability challenges by storing large datasets externally while maintaining verifiable references on the blockchain. The workflow emphasizes the role of distributed consensus mechanisms in ensuring transaction legitimacy and preventing unauthorized modifications. By recording transaction hashes on an immutable ledger, the system enables transparent and tamper-proof data verification. The integration of blockchain with traditional architecture offers significant advantages, including decentralization, enhanced security, and improved auditability. However, challenges such as scalability, latency, and interoperability remain areas for further research. Overall, the proposed blockchain-integrated system provides a comprehensive framework for secure and transparent data transactions, making it suitable for applications across various domains, including finance, healthcare, and supply chain management.

Corresponding Author:

Name: Wajihi Ali
Institution: Institute of Educational and Management Technologies, the Open University of Tanzania, Kinondoni, Tanzania
Email: wajihiali089@gmail.com

1. INTRODUCTION

The rapid digital transformation of modern societies has led to an unprecedented growth in data generation, storage, and exchange. From financial transactions and healthcare records to supply chain management and Internet of Things (IoT) systems, data has become a critical asset that drives decision-making and operational efficiency. However, the increasing reliance

on digital systems has also exposed significant challenges related to data security, integrity, transparency, and trust [1]–[3]. Traditional centralized architectures, which depend on a single authority for data validation and storage, are particularly vulnerable to cyberattacks, data breaches, and unauthorized manipulation [4]. These limitations have created a pressing need for more robust and trustworthy system architectures.

Blockchain technology has emerged as a promising solution to address these challenges. Initially introduced as the underlying technology for Bitcoin, blockchain is a decentralized, distributed ledger that records transactions in a secure and immutable manner [5]. Unlike conventional systems, blockchain eliminates the need for intermediaries by enabling peer-to-peer transactions that are validated through consensus mechanisms. This decentralized approach enhances transparency, reduces the risk of single points of failure, and ensures that data cannot be altered once recorded. The integration of blockchain into system architecture represents a significant advancement in the design of secure and transparent data transaction systems. A blockchain-integrated system architecture combines traditional computing layers—such as user interfaces and application services—with decentralized ledger technology, cryptographic mechanisms, and distributed storage solutions. This hybrid approach leverages the strengths of both centralized and decentralized systems, enabling efficient data processing while maintaining high levels of security and trust [6].

One of the key features of blockchain technology is its ability to ensure data integrity through cryptographic hashing. Each transaction recorded on the blockchain is associated with a unique hash value, which serves as a digital fingerprint. Any attempt to modify the data results in a change in the hash value, making tampering easily detectable. Additionally, the use of digital signatures ensures that transactions are authenticated and cannot be repudiated by the sender [7]. These features make blockchain particularly suitable for applications where data authenticity and traceability are critical. Another important aspect of blockchain-integrated systems is the use of smart contracts. Smart contracts are self-executing programs that automatically enforce predefined rules and conditions. They enable automation of complex processes, reduce human intervention, and minimize the risk of errors or fraud [8]. For example, in a supply chain system, a smart contract can automatically trigger payment once goods are delivered and verified, thereby improving efficiency and transparency.

Despite its advantages, blockchain technology also faces several challenges, including scalability, energy consumption, and integration with existing systems. Public blockchain networks often struggle to handle high transaction volumes, leading to delays and increased costs [9]. To address these issues, researchers have proposed various solutions, such as off-chain storage, layer-2 scaling techniques, and alternative consensus mechanisms. In this context, the concept of blockchain-integrated system architecture becomes crucial. By incorporating off-chain storage solutions, such as cloud databases or decentralized file systems like IPFS, the architecture can efficiently handle large datasets while maintaining data integrity through blockchain-based verification [10]. Similarly, the adoption of energy-efficient consensus mechanisms, such as Proof of Stake (PoS), can reduce computational overhead and improve system performance.

The primary objective of this study is to explore a blockchain-integrated system architecture that ensures secure and transparent data transactions. The proposed architecture aims to address the limitations of traditional systems by leveraging blockchain technology to enhance data security, integrity, and traceability. It also seeks to provide a scalable and efficient framework that can be applied across various domains. In summary, blockchain technology has the potential to revolutionize the way data transactions are managed by providing a decentralized, secure, and transparent framework. The integration of blockchain into

system architecture represents a significant step toward building trustworthy digital ecosystems. As research and development in this field continue to advance, blockchain-integrated systems are expected to play a pivotal role in shaping the future of data management.

2. LITERATURE REVIEW

The application of blockchain technology in secure data transaction systems has been widely studied in recent years. Researchers have explored various aspects of blockchain, including its architecture, consensus mechanisms, security features, and integration with other technologies. This section reviews the existing literature to provide a comprehensive understanding of the current state of research in blockchain-integrated systems. [5] introduced blockchain as a decentralized digital ledger for peer-to-peer electronic cash transactions. The Bitcoin system demonstrated how cryptographic techniques and consensus mechanisms could be used to achieve secure and trustless transactions without the need for intermediaries. This foundational work laid the groundwork for subsequent research on blockchain technology and its applications.

Following Nakamoto's work, researchers have examined the broader implications of blockchain beyond cryptocurrency. [9] provided an overview of blockchain architecture, highlighting its key components, including distributed ledgers, consensus mechanisms, and cryptographic algorithms. The study emphasized the potential of blockchain to improve transparency and security in various applications, while also identifying challenges related to scalability and performance.

The integration of blockchain with IoT systems has also received significant attention. [11] explored how blockchain and smart contracts can enhance the security and reliability of IoT networks. They argued that blockchain can provide a decentralized framework for managing IoT data, ensuring data integrity and preventing unauthorized access. However, they also noted the limitations of blockchain in handling large volumes of IoT data, suggesting the need for hybrid architectures that combine blockchain with off-chain storage.

Another important area of research is the use of smart contracts in blockchain systems. [8] introduced Ethereum as a platform for developing decentralized applications (DApps) using smart contracts. This innovation expanded the capabilities of blockchain by enabling programmable transactions and automated processes. Smart contracts have since been widely adopted in various domains, including finance, supply chain management, and healthcare.

Security is a critical aspect of blockchain-integrated systems, and several studies have focused on analyzing its strengths and vulnerabilities. [7] examined the security properties of Bitcoin and identified potential risks, such as double-spending attacks and mining centralization. Their work highlighted the importance of robust consensus mechanisms and network design in ensuring system security.

The scalability of blockchain systems has been a major concern in the literature. [6] discussed architectural approaches for improving blockchain scalability, including sharding, sidechains, and layer-2 solutions. These approaches aim to increase transaction throughput while maintaining security and decentralization. Similarly, [12] conducted a systematic review of blockchain applications and identified scalability as one of the key challenges limiting widespread adoption. The use of off-chain storage solutions has been proposed as a way to address storage limitations. [10] introduced the Interplanetary File System (IPFS), a decentralized storage system that uses content-addressing to store and retrieve data. By integrating IPFS with blockchain, researchers have developed hybrid architectures that combine the benefits of decentralized storage and secure data verification.

In the context of supply chain management, [13] explored the role of blockchain in enhancing transparency and traceability. Their study demonstrated how blockchain can provide a secure and

immutable record of transactions, enabling stakeholders to track the movement of goods and verify their authenticity. This application highlights the potential of blockchain to improve trust and efficiency in complex systems. Recent research has also focused on privacy-enhancing techniques in blockchain systems. Techniques such as zero-knowledge proofs and homomorphic encryption allow data to be verified without revealing sensitive information, addressing concerns related to data confidentiality [12]. These advancements are particularly important for applications in healthcare and finance, where privacy is a critical requirement.

3. BLOCKCHAIN-INTEGRATED SYSTEM ARCHITECTURE

Blockchain technology has significantly transformed the landscape of secure data management by introducing decentralized, transparent, and tamper-resistant systems. Unlike traditional centralized architectures, where a single authority controls data storage and validation, blockchain distributes these responsibilities across a network of nodes, thereby enhancing trust and resilience [5]. This paradigm shift is particularly relevant in domains where data integrity, traceability, and security are critical, such as financial systems, healthcare records, supply chains, and Internet of Things (IoT) ecosystems.

Figure 1 illustrates a blockchain-integrated system architecture designed to facilitate secure and transparent data transactions. The architecture adopts a layered approach that integrates conventional computing components with blockchain technology. Each layer—user, application, blockchain, off-chain storage, and security—performs a distinct function while collectively contributing to the system's robustness. By combining decentralization with efficient data handling mechanisms, the architecture addresses limitations of both traditional systems and standalone blockchain implementations.

3.1 User Layer

The user layer serves as the primary interface between end users and the system. It encompasses various client-side platforms such as web applications, mobile applications, and IoT devices. These interfaces enable users to initiate transactions, submit data, and retrieve information from the system.

In practical implementations, user interactions are often facilitated through intuitive graphical interfaces that hide the complexity of blockchain operations. For instance, a user submitting a document through a web application may not be aware that the system generates a cryptographic hash and records it on a blockchain. Similarly, IoT devices continuously generate data streams, which are securely transmitted and processed without manual intervention.

Authentication mechanisms, such as public-private key cryptography, are typically employed at this layer to ensure that only authorized users can access system functionalities. Each user possesses a unique cryptographic identity, which is used to sign transactions and verify ownership. This approach enhances accountability and prevents unauthorized access [4].

Overall, the user layer is responsible for initiating system interactions while ensuring secure communication with underlying components.

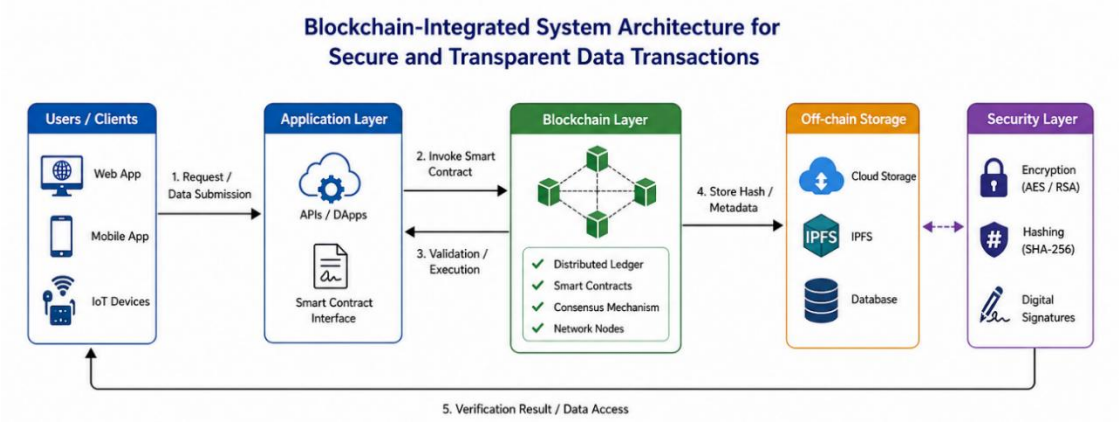

Figure 1. Blockchain-Integrated System Architecture for Secure and Transparent Data Transactions

3.2 *Application Layer*

The application layer acts as an intermediary between the user layer and the blockchain network. It includes application programming interfaces (APIs), decentralized applications (DApps), and smart contract interfaces that facilitate communication and data processing.

DApps are software applications that operate on decentralized networks rather than centralized servers. They leverage blockchain technology to ensure transparency and reliability. Unlike traditional applications, DApps interact directly with smart contracts, which define the logic governing transactions. Smart contracts are self-executing programs stored on the blockchain that automatically enforce predefined rules when certain conditions are met [8].

3.3 *Blockchain Layer*

The blockchain layer forms the core of the architecture, providing a decentralized and immutable ledger for recording transactions. This layer consists of distributed nodes that collectively validate and store transaction data.

3.4 *Distributed Ledger*

A distributed ledger is a synchronized database shared across multiple nodes in a network. Each node maintains a copy of the ledger, ensuring redundancy and fault tolerance. This decentralized structure eliminates the risk of a single point of failure and enhances data availability. Transactions recorded on the ledger are organized into blocks, which are cryptographically linked to form a chain. Once a block is added, it becomes extremely difficult to alter its contents, ensuring data integrity [5].

3.5 *Smart Contracts*

Smart contracts play a crucial role in automating processes within the blockchain layer. These contracts are written in programming languages such as Solidity and deployed on blockchain platforms like Ethereum. Once deployed, they execute automatically when predefined conditions are satisfied, reducing the need for intermediaries and minimizing human error [14].

Smart contracts also enhance transparency, as their code and execution are visible to all participants in the network.

3.6 *Consensus Mechanisms*

Consensus mechanisms ensure that all nodes in the network agree on the validity of transactions before they are added to the ledger. Common mechanisms include Proof of Work (PoW), Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT). For instance, PBFT is particularly suitable for permissioned blockchain systems, as it provides high throughput and low latency while tolerating malicious nodes [15]. These mechanisms prevent double-

spending and ensure that only legitimate transactions are recorded.

3.7 Network Nodes

Nodes are the fundamental units of the blockchain network. They validate transactions, maintain the ledger, and participate in consensus processes. The decentralized nature of nodes enhances system resilience, as the failure of a single node does not compromise the entire network. Together, these components ensure that the blockchain layer provides a secure, transparent, and tamper-proof environment for data transactions.

4. OFF-CHAIN STORAGE LAYER

While blockchain ensures data integrity and immutability, it is not designed for storing large volumes of data due to scalability and cost constraints. To address this limitation, the architecture incorporates an off-chain storage layer. This layer includes cloud storage systems, traditional databases, and decentralized storage solutions such as the InterPlanetary File System (IPFS). These systems store the actual data, while the blockchain stores only a cryptographic hash or reference to that data. IPFS, for example, uses content-addressing to store and retrieve data, ensuring that files are uniquely identified by their cryptographic hash. This approach enhances data integrity and availability [10].

The security layer operates across all components of the architecture, providing mechanisms to protect data confidentiality, integrity, and authenticity. Researchers are actively exploring solutions such as sharding, layer-2 scaling, and alternative consensus mechanisms to address these challenges [6]. Encryption ensures that sensitive data remains confidential during transmission and storage. Techniques such as Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA) are widely used to secure data against unauthorized access.

Hashing algorithms, such as SHA-256, generate fixed-length outputs from input data. These outputs serve as digital fingerprints, enabling the detection of any changes to the original data. Even a minor alteration results in a completely different hash, making tampering easily identifiable [4]. Digital signatures provide authentication and non-repudiation. By signing transactions with private keys, users can prove their identity and ensure that transactions cannot be altered after submission. The integration of these techniques ensures a robust security framework that protects the system from various cyber threats.

5. DATA FLOW IN THE ARCHITECTURE

The architecture follows a systematic data flow process. Initially, users submit data through the user layer. The application layer processes this data and interacts with smart contracts to initiate transactions. These transactions are then broadcast to the blockchain network, where nodes validate them using consensus mechanisms. Once validated, the transaction is recorded on the blockchain, and a hash of the data is stored. The actual data is stored in the off-chain storage layer. When users need to access the data, they retrieve it from off-chain storage and verify its integrity by comparing its hash with the one stored on the blockchain. The architecture offers several advantages, including enhanced transparency, improved security, and decentralized control. It enables organizations to maintain trustworthy systems without relying on centralized authorities.

However, challenges such as scalability, latency, and energy consumption remain significant concerns. Ongoing research focuses on optimizing consensus mechanisms and integrating hybrid storage solutions to overcome these limitations.

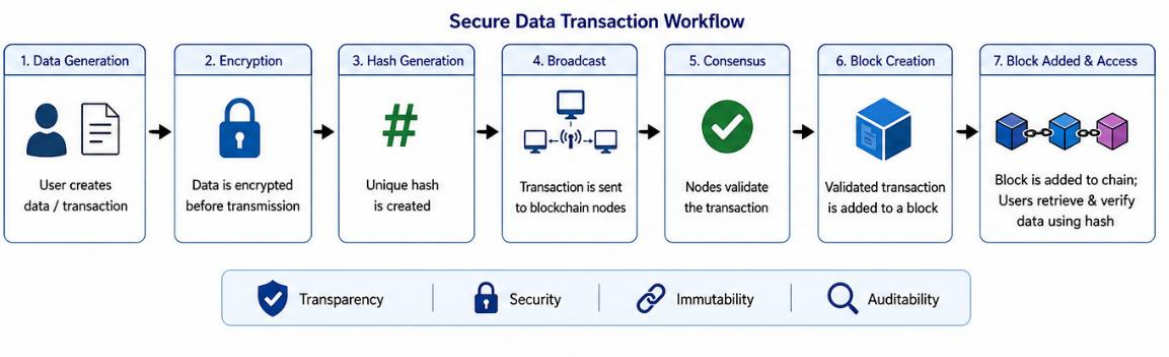

Figure 2. Secure Data Transaction Workflow Using Blockchain

The rapid growth of digital ecosystems has intensified the need for secure, transparent, and reliable mechanisms for data transactions. Traditional centralized systems often rely on trusted intermediaries to validate and store data, which introduces vulnerabilities such as single points of failure, data breaches, and lack of transparency. Blockchain technology addresses these challenges by offering a decentralized and immutable ledger that ensures data integrity and trust among participants [5], [9].

Figure 2 illustrates a secure data transaction workflow enabled by blockchain technology. This workflow demonstrates how data progresses through multiple stages from generation and encryption to validation and verification assuring confidentiality, integrity, and transparency. By leveraging cryptographic primitives, distributed consensus, and decentralized storage, blockchain provides a robust framework for managing digital transactions across diverse domains such as finance, healthcare, and supply chain management [12]. At this stage, it is essential to ensure the authenticity and accuracy of the generated data. Metadata such as timestamps, user identity, and transaction context are typically included to provide traceability. In blockchain-enabled systems, this metadata plays a crucial role in establishing accountability and enabling audit trails [11]. Symmetric encryption methods, such as AES, are commonly used for their efficiency in handling large datasets, while asymmetric encryption techniques, such as RSA or elliptic curve cryptography (ECC), are employed for secure key exchange and digital signatures [16].

6. LIMITATIONS

Despite the transformative potential of blockchain-integrated systems in enabling secure and transparent data transactions, several limitations continue to impede their large-scale adoption. One of the most significant challenges is scalability. Public blockchain networks, such as Bitcoin and Ethereum, process transactions at a much lower rate compared to traditional centralized systems. This limitation stems from the requirement that every transaction must be validated by multiple nodes through consensus mechanisms, which introduces computational overhead and slows down throughput [9]. As network usage increases, congestion can lead to higher transaction costs and delays, making blockchain less practical for high-frequency applications such as real-time financial processing or large-scale IoT deployments [6].

Another critical limitation is latency and performance inefficiency. Blockchain systems inherently require time to validate and confirm transactions, particularly in consensus models like Proof of Work (PoW), where miners must solve complex cryptographic puzzles [5]. Even more efficient consensus mechanisms, such as Proof of Stake (PoS) or Practical Byzantine Fault Tolerance (PBFT), still involve communication overhead among distributed nodes. These delays can be problematic for applications that demand near-instantaneous responses, such as healthcare monitoring systems or automated trading platforms [12].

Energy consumption is also a major concern, especially in PoW-based systems.

Mining operations require significant computational power, resulting in high electricity usage and environmental impact. Studies have highlighted that blockchain networks like Bitcoin consume energy comparable to that of small nations, raising sustainability concerns [7]. Although alternative consensus mechanisms aim to reduce energy consumption, achieving a balance between efficiency, security, and decentralization remains a challenge.

In addition, privacy and data confidentiality present notable issues. While blockchain promotes transparency by making transaction records publicly accessible, this feature can conflict with the need to protect sensitive information. Even when data is encrypted, transaction metadata—such as timestamps and user activity patterns—can potentially expose user behavior [12]. This limitation is particularly critical in domains like healthcare and finance, where strict data protection regulations must be adhered to.

Storage limitations further complicate blockchain implementation. Since each node maintains a copy of the entire ledger, the size of the blockchain grows continuously over time. This growth can strain storage resources and reduce system efficiency. Storing large datasets directly on-chain is impractical due to cost and performance constraints, necessitating the use of off-chain storage solutions [10]. However, integrating off-chain storage introduces additional complexity and potential vulnerabilities. Another key limitation is interoperability. Many blockchain platforms operate in isolation, lacking standardized protocols for communication with other systems. This fragmentation restricts the seamless exchange of data and assets across different blockchain networks and limits the overall scalability of the ecosystem [6]. Without effective interoperability, organizations may face challenges in integrating blockchain solutions into broader digital infrastructures.

Finally, integration with legacy systems poses significant technical and organizational barriers. Existing enterprise systems are often built on centralized architectures that are not inherently compatible with decentralized blockchain frameworks. Transitioning to blockchain requires substantial modifications to infrastructure, processes, and governance models. Additionally, the lack of standardized implementation frameworks and skilled professionals further complicates adoption [13].

7. FUTURE DIRECTIONS

To address these limitations, ongoing research and development efforts are focused on advancing blockchain technology in several key areas. One of the most promising directions is the development of scalability solutions. Techniques such as sharding, which divides the blockchain network into smaller partitions for parallel transaction processing, have shown potential in increasing throughput [9]. Similarly, layer-2 solutions, such as payment channels and sidechains, enable off-chain transaction processing while maintaining the security of the main blockchain. These innovations aim to enhance performance without compromising decentralization.

Another important area of advancement is the adoption of energy-efficient consensus mechanisms. Alternatives to PoW, such as Proof of Stake (PoS), Delegated Proof of Stake (DPoS), and Proof of Authority (PoA), significantly reduce computational requirements and energy consumption (Xu et al., 2019). These mechanisms improve sustainability while maintaining security and efficiency, making blockchain more environmentally viable for widespread use.

Privacy-enhancing technologies are also gaining attention as a means to address confidentiality concerns. Techniques such as zero-knowledge proofs (ZKPs), homomorphic encryption, and secure multi-party computation (SMPC) allow data to be verified without revealing sensitive information [12]. For example, zero-knowledge proofs enable one party to prove the validity of a statement without disclosing the underlying data, thereby balancing transparency and privacy. Improving

interoperability is another critical focus area. Cross-chain communication protocols and blockchain bridges are being developed to facilitate the exchange of data and assets between different blockchain networks. These solutions aim to create a more interconnected ecosystem where multiple blockchains can operate seamlessly together [6]. Standardization efforts by industry consortia and research organizations are expected to play a vital role in achieving this goal. Following encryption, a cryptographic hash of the data is generated. Hash functions, such as SHA-256, produce a fixed-length output that uniquely represents the input data. This output serves as a digital fingerprint, enabling the detection of any changes to the original data [5].

The properties of hash functions determinism, collision resistance, and pre-image resistance—make them ideal for ensuring data integrity. Even a minor modification in the input data results in a completely different hash value, making tampering easily detectable [7]. Transactions are digitally signed using the sender's private key, ensuring authenticity and non-repudiation. Digital signatures allow network participants to verify the identity of the sender and confirm that the transaction has not been altered [14]. Broadcasting ensures that the transaction is distributed across the network, promoting transparency and decentralization. Unlike centralized systems, where a single entity controls transaction processing, blockchain distributes this responsibility among multiple participants [9]. PBFT is particularly effective in permissioned blockchain systems, offering high throughput and low latency [15]. Consensus mechanisms prevent issues such as double-spending and ensure that only legitimate transactions are recorded [6].

The inclusion of the previous block's hash creates a chain-like structure, linking all blocks together. This design ensures that any attempt to alter a block would require modifying all subsequent blocks, which is computationally infeasible [5]. The addition of blocks is irreversible, ensuring data immutability. This property is a key advantage of blockchain technology, as it prevents unauthorized modifications and ensures long-term data integrity [12]. This mechanism provides a reliable method for ensuring data authenticity and is widely used in applications requiring auditability and compliance, such as financial auditing and supply chain tracking [13].

The integration of blockchain with emerging technologies such as artificial intelligence (AI), Internet of Things (IoT), and cloud computing presents additional opportunities for innovation. For instance, blockchain can enhance the security and trustworthiness of IoT data by providing immutable records, while AI can optimize decision-making processes within blockchain networks and even in agritech Systems [1], [11]. Such integrations are expected to enable the development of intelligent, autonomous systems capable of handling complex data transactions.

8. CONCLUSION

This study presents a comprehensive blockchain-integrated system architecture for enabling secure and transparent data transactions, supported by detailed architectural and workflow representations. The proposed framework demonstrates how blockchain technology can be effectively combined with traditional system components to address critical challenges associated with data security, integrity, and trust. This integration enables efficient data processing while ensuring that sensitive information is protected through encryption and cryptographic hashing. The use of off-chain storage further enhances system scalability by allowing large datasets to be managed efficiently without overloading the blockchain. It outlines the sequential steps involved in processing a transaction, including data generation, encryption, hash creation, consensus validation, block formation, and final verification. This workflow underscores the importance of decentralized consensus mechanisms in maintaining data integrity and preventing unauthorized modifications. The combined insights from both figures demonstrate that

blockchain technology offers a robust solution for achieving transparency and immutability in data transactions. By eliminating reliance on centralized authorities, the proposed system enhances trust among participants and enables reliable audit trails. In conclusion, the proposed architecture and workflow provide a strong foundation for developing secure, transparent, and efficient data transaction systems, positioning blockchain as a key technology in the evolution of modern digital infrastructures.

FUNDING

This research received no external funding.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] Md. Ishtiaque Alam, Mohammad Abdus Sami, Md Abu Kawsar Prodhan Hemal, and Md Lutfor Rahman, "Predictive Analytics and Decision Intelligence for Climate-Resilient Agritech Systems," *Acad. Glob. J. Comput. Sci. Technol. Stud.*, vol. 2, no. 1 SE-Research Article, pp. 44–56, 2023, doi: 10.32996/agjcsts.2023.2.1.4.

[2] T. R. Sikder, M. A. Siam, M. M. H. Melon, S. M. M. Uddin, S. C. Mohonta, and F. Karim, "A Multimodal Data Analytics Framework for Early Cancer Detection Using Genomic, Radiomic, and Clinical Big Data Fusion," *J. Comput. Sci. Technol. Stud.*, vol. 5, no. 3, pp. 183–188, 2023.

[3] B. J. A. Juie, J. U. Z. Kabir, R. A. Ahmed, and M. M. Rahman, "Evaluating the impact of telemedicine through analytics: Lessons learned from the COVID-19 era," *J. Med. Heal. Stud.*, vol. 2, no. 2, pp. 161–174, 2021.

[4] W. Stallings, *Cryptography and network security: Principles and practice*, 7th ed. Pearson, 2017.

[5] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Available SSRN 3440802*, 2008.

[6] X. Xu, I. Weber, and M. Staples, "Architecture for blockchain applications," 2019.

[7] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in *2015 IEEE symposium on security and privacy*, 2015, pp. 104–121.

[8] V. Buterin, "A next-generation smart contract and decentralized application platform," *white Pap.*, vol. 3, no. 37, pp. 1–2, 2014.

[9] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE international congress on big data (BigData congress)*, 2017, pp. 557–564.

[10] J. Benet, "Ipfs-content addressed, versioned, p2p file system," *arXiv Prepr. arXiv1407.3561*, 2014.

[11] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE access*, vol. 4, pp. 2292–2303, 2016.

[12] F. Casino, T. K. Dasaklis, and C. Patsakis, "A systematic literature review of blockchain-based applications: Current status, classification and open issues," *Telemat. informatics*, vol. 36, pp. 55–81, 2019.

[13] S. Saberi, M. Kouhizadeh, J. Sarkis, and L. Shen, "Blockchain technology and its relationships to sustainable supply chain management," *Int. J. Prod. Res.*, vol. 57, no. 7, pp. 2117–2135, 2019.

[14] N. Szabo, "Formalizing and securing relationships on public networks," *First monday*, 1997.

[15] M. Castro and B. Liskov, "Practical byzantine fault tolerance," in *OsDI*, 1999, vol. 99, no. 1999, pp. 173–186.

[16] R. Kahn and R. Wilensky, "A framework for distributed digital object services," *Int. J. Digit. Libr.*, vol. 6, no. 2, pp. 115–123, 2006.