A Study on Blockchain-Driven IoT Payment Systems

Maimunatu Ya'u Ibrahim
Department of Management and Information Technology, Abubakar Tafawa Balewa University, Bauchi
yimaimunatu.pg@atbu.edu.ng

Kabiru Ibrahim Musa
Department of Management and Information Technology, Abubakar Tafawa Balewa University, Bauchi
imkabir@atbu.edu.ng

Aminu Ahmad
Department of Management and Information Technology, Abubakar Tafawa Balewa University, Bauchi
aminuahmad@atbu.edu.ng

Muhammad Tella
Department of Management and Information Technology, Abubakar Tafawa Balewa University, Bauchi
tmuhammad@atbu.edu.ng

***Abstract*— Blockchain technology has emerged as a transformative innovation capable of reshaping digital financial services, particularly in the era of the Internet of Things (IoT). While IoT enables real-time connectivity and service delivery, its centralized architecture exposes systems to risks such as data breaches, single points of failure, and limited transparency. This study addresses these challenges by developing a conceptual hybrid framework that integrates blockchain with IoT to strengthen the security, scalability, and regulatory compliance of digital payment systems. The paper reviews existing blockchain architectures, consensus algorithms, and IoT vulnerabilities to identify the functional gaps limiting current financial applications. The proposed conceptual framework combines IoT's real-time data acquisition with blockchain's distributed ledger, cryptographic validation, and smart contracts to enhance transaction integrity and automate payment processes. A comparative analysis of consensus mechanisms (PoA, PoS, PBFT) demonstrates the suitability of permissioned blockchains for financial environments requiring efficient and compliant operations. The research adopts a theoretical design approach, outlining the framework's architecture, design assumptions, and limitations. While the model has not been empirically tested, it provides a foundation for future prototype development and performance validation in real-world banking contexts. The findings suggest that integrating blockchain's decentralization and immutability with IoT infrastructures can significantly improve the security, transparency, and efficiency of next-generation financial systems.**

Keywords: **Blockchain, IoT, Payment System, Security, Hybrid-Conceptual Framework.**

I. INTRODUCTION

The global financial ecosystem is undergoing a rapid transformation driven by emerging technologies such as the Internet of Things (IoT), artificial intelligence, and blockchain. Among these, blockchain is widely regarded as the next disruptive innovation after the Internet, offering decentralized, transparent, and tamper-resistant transaction management. Initially developed as the underlying technology for Bitcoin, blockchain has since evolved to support diverse applications across banking, supply chain, healthcare, and governance.

IoT, on the other hand, connects billions of devices and facilitates real-time data exchange, enabling innovative services such as wearable-based payments, smart contracts, and automated financial transactions. However, the centralized nature of many IoT architectures raises concerns regarding data security, privacy, and resilience. Centralized servers represent single points of failure, creating vulnerabilities to cyberattacks and unauthorized access. Integrating blockchain with IoT offers a promising solution to these challenges. Blockchain's distributed ledger architecture ensures immutable and transparent records of financial transactions, while consensus algorithms and smart contracts facilitate efficiency and trust.

While many global industries have adopted blockchain, its integration into IoT-based financial systems particularly in developing contexts remains underexplored. This research seeks to bridge that gap by examining how blockchain's core features can enhance the security, scalability, and transparency of IoT-driven payment infrastructures. Recent studies emphasize the advantages of permissioned blockchains in the financial sector, where controlled access, high transaction throughput, and regulatory compliance are critical.

This paper examines blockchain's core features, capabilities, and applications in the context of digital banking, with particular attention to its role in enhancing IoT-based payment systems. A hybrid IoT–Blockchain framework is proposed to address scalability, privacy, and security concerns while supporting real-time and high-volume financial operations.

This paper examines blockchain's core features, capabilities, and applications in the context of digital banking, with particular attention to its role in enhancing IoT-based payment systems. A conceptual hybrid IoT–Blockchain framework is proposed to address scalability, privacy, and security concerns while supporting real-time and high-volume financial operations. The remainder of this paper is structured as follows: Section II reviews blockchain technology and analyzes its key properties in addressing IoT payment vulnerabilities. Section III presents the different types of blockchain networks and justifies the adoption of permissioned blockchains for financial applications. Section IV outlines the capabilities and practical applications of blockchain across sectors, followed by a discussion of its role in IoT payment systems in Section V. Section VI introduces the proposed conceptual framework and its methodological design rationale. Section VII provides a comparative evaluation of consensus mechanisms and highlights the performance suitability of Proof of Authority (PoA). Section VIII discusses the findings, practical deployment constraints, and implementation challenges. Finally, Section IX concludes the paper and suggests directions for future research.

II. LITERATURE REVIEW

Blockchain technology provides a decentralized ledger system that records transactions securely across a distributed network of nodes. Its core properties include immutability, decentralization, transparency, cryptographic security, and consensus mechanisms which directly address the primary vulnerabilities of IoT-based payment systems [1].

IoT payment infrastructures often rely on centralized servers, which create single points of failure and expose sensitive financial data to cyberattacks and unauthorized access. Blockchain's decentralization removes this structural weakness by distributing data storage and validation across multiple nodes, ensuring continuity even if parts of the network are compromised [2].

The immutability of blockchain transactions, enforced through cryptographic hashing and chained block structures, mitigates risks of data tampering and fraudulent manipulation which is a persistent concern in IoT payments where devices generate continuous streams of sensitive data [3]. Furthermore, transparency within a permissioned blockchain enables traceability and auditability of transactions without compromising privacy. This property enhances accountability among financial actors and facilitates regulatory compliance [4].

Consensus mechanisms such as Proof of Authority (PoA) or Practical Byzantine Fault Tolerance (PBFT) ensure the integrity and validation of transactions without excessive computational cost which is a critical advantage in IoT environments that require lightweight and energy-efficient solutions [5]. Finally, smart contracts automate transaction verification and execution, reducing dependency on intermediaries and eliminating latency associated with manual reconciliation. This improves transaction throughput and operational efficiency, two essential factors in real-time IoT payment scenarios.

In summary, blockchain's distributed architecture transforms the security and reliability landscape of IoT-based financial systems. By combining decentralization for resilience, immutability for integrity, and consensus for trust, blockchain establishes a secure foundation for scalable digital payments in interconnected IoT environments [6].

A. Types of Blockchain

Blockchain technology has evolved into multiple forms to serve a range of needs across industries. Broadly, blockchain networks are categorized into four major types: public, private, consortium (also known as federated), and hybrid blockchains. Each type differs in governance structure, degree of decentralization, accessibility, and suitability for particular applications.

Public blockchains, also referred to as permissionless blockchains, are completely open and decentralized. In these networks, anyone can join, read data, initiate transactions, and participate in the consensus process that validates new blocks. They rely on cryptographic consensus mechanisms such as Proof of Work (PoW) or Proof of Stake (PoS) to achieve trust without intermediaries. Public blockchains are best known for their use in cryptocurrency systems like Bitcoin and Ethereum, where transparency, immutability, and resistance to censorship are key priorities [7]. However, public blockchains often face limitations in transaction throughput, scalability, latency, and energy efficiency due to the computationally intensive nature of their consensus algorithms. These constraints make them less ideal for environments where speed, privacy, or regulatory control is required such as financial institutions or IoT-based payment systems.

In contrast, private blockchains, also known as permissioned blockchains, are operated by a single organization that controls access to the network. Only selected participants can read or write to the blockchain, and consensus is typically achieved through more lightweight protocols such as Practical Byzantine Fault Tolerance (PBFT) or Proof of Authority (PoA). These blockchains offer improved performance, better privacy controls, and are more energy-efficient compared to their public counterparts [8]. As such, private blockchains are widely used in enterprise environments, including supply chain management, healthcare, and internal banking systems.

Consortium blockchains offer a middle ground between the transparency of public networks and the control of private ones. In a consortium blockchain, multiple trusted organizations share responsibilities for maintaining the blockchain and validating transactions. This model is particularly useful in sectors where collaboration among known entities is essential such as in interbank clearing systems, trade finance, and insurance claim processing [9]. Consortium blockchains promote shared governance while retaining privacy and performance benefits. For example, a group of banks can jointly operate a consortium blockchain to streamline cross-border payments, reducing the need for third-party intermediaries while ensuring mutual trust.

Hybrid blockchains integrate the characteristics of both permissioned and permissionless networks. These systems allow certain data and functionalities to remain public while restricting access to sensitive operations or information. Hybrid models are particularly useful in contexts like government services, real estate, healthcare, and IoT platforms, where selective transparency is crucial. In IoT applications, hybrid blockchains can enable secure device-to-device communication, maintain data privacy, and ensure real-time payment processing while still supporting traceability and auditability for external oversight [10]. By combining the benefits of both open and closed systems, hybrid blockchains provide flexibility and adaptability for complex digital environments.

The selection of blockchain type depends largely on the specific needs of the use case, including trust requirements, performance expectations, privacy concerns, and regulatory constraints. In the context of this thesis, which focuses on developing a secure and scalable digital banking payment system integrated with IoT infrastructure, a permissioned blockchain specifically, a private blockchain was adopted. This choice is informed by the need for controlled access, efficient processing, and high transaction throughput, which are essential in financial systems handling sensitive data and real-time operations. Private blockchains mitigate the scalability limitations often observed in traditional public blockchains, such as network congestion, high latency, and excessive energy consumption. By allowing a smaller group of trusted nodes to validate transactions using lightweight consensus algorithms like PoA, private blockchains support faster and more scalable operations without compromising security [11]. This makes them particularly suitable for IoT-based digital banking platforms where speed, data integrity, and resource efficiency are critical.

B. Blockchain Capabilities

This is going to outline the capabilities of blockchain technology, having the first objective of the study seeking to examine the security capabilities of blockchain technology on the performance

of the IoT-based payment system. The blockchain capabilities will further serve as a basis for building the research questionnaire.

While blockchain technology offers a range of applications, its core benefit lies in reducing reliance on a trusted third party. Traditionally, interactions with other businesses or individuals have required a degree of trust, often established through third-party certifications or the reputation of the entity involved. Blockchain, however, shifts this trust from individual entities to the technology itself, providing an alternative solution [12]. Blockchain, as a distributed ledger, enables consensus mechanisms in trustless networks while offering flexible levels of privacy and anonymity. It also supports smart contracts, which automate transactions through multiple layers of validation within a transparent framework. Crucially, once recorded, blockchain transactions are immutable and resistant to alteration, ensuring a tamper-proof audit trail. Together, these features position blockchain as a powerful solution for secure and decentralized transaction management [4]: Trustless: Information is controlled by the parties involved, and exchanges between them can take place without the involvement of a reliable third party. Integrity: Transactions are carried out precisely as instructed by the protocol. Transparency: By making modifications to public blockchains available to all entities for analysis and access, transparency is established. Good data: All of the data on the blockchain is accurate, unified, and unchangeable. Reliability: The decentralized network that blockchain employs removes the risk of a single point of failure and increases resistance against assaults.

C. Blockchain Applications

Legal papers, health data, supply chains, IoT e-business, the energy market, e-government, decentralized registries, stock exchanges, and smart cities have all included blockchain technology as a means of proving their existence. Contracts, transactions, and records are dealt with by the legal, political, and economic systems. They impose organizational constraints and safeguard resources. They produce information and verify it. Interactions between nations, cultures, businesses, and people are made possible by this knowledge. Any system or organization may take use of the blockchain technology's capability to transfer information between participants in a transparent and safe manner [3].

FinTech companies are increasingly exploring cryptocurrency and exchange markets, as well as investigating how blockchain technology can support business-to-business transactions. These investigations highlight potential benefits such as reducing counterparty risks, enhancing cybersecurity, and improving transparency [4]. In the healthcare sector, for example, patient records and medical research data need to be shared in a way that ensures both privacy and data integrity.

Similarly, blockchain technology can be utilized in organizations responsible for civil registries, including records of deaths, marriages, and land ownership. Meanwhile, the energy sector is exploring blockchain as a solution to the high costs of maintaining centralized systems and the challenge of managing large volumes of transactional and analytical data. A peer-to-peer blockchain approach could help mitigate these issues. As the IoT continues to expand, it offers a wide range of services and applications. Developing complementary technologies and frameworks can harness the strengths of each technology to foster innovation and synergy [2].

D. Blockchain In Banking and Fintech Industries

The blockchain system operates as a decentralized digital ledger accessible via the internet and shared among all network participants. Before being permanently recorded, transactions and events undergo validation to ensure accuracy and consensus. This architecture allows users to securely exchange and access data without the need for mutual trust, as the ledger is immutable and resistant to tampering. Consequently, no single entity holds exclusive control over the vast data generated by IoT devices. By enabling users to view and trace past transactions, blockchain fosters transparency and facilitates the swift identification and resolution of data breaches. With its "security by design" principle, blockchain effectively addresses critical security concerns in IoT ecosystems. It is transforming various domains from financial transactions to fundraising in the private sector by eliminating the need for centralized intermediaries and enabling decentralized application deployment [5].

Industry 4.0 integrates IoT, cloud computing, artificial intelligence, and blockchain to advance automation in industrial processes [13]. IoT usage is growing, yet there are scalability, safety, secrecy, and reliability challenges. Originally designed to manage cryptocurrencies, blockchain has been integrated with IoT to enhance it due to its decentralized nature, greater safety, integrity, security, and privacy. Blockchain technology also enhances the system infrastructure of many IoT devices, making it more effective for supporting IoT devices, especially in terms of transaction speed.

Before, it was difficult to complete the process without compromising either efficiency or security. IoT design issues may be solved using blockchain features including immutability, transparency, auditability, data encryption, and operational resilience, claim. The basic objective of the blockchain is to free individuals from any reliance on the intermediaries who currently "manage" and "control" a sizable chunk of individuals' lives. The original use of blockchain knowledge was to expedite transactions using Bitcoin, a brand-new kind of decentralized, bank- and government-free money. This digital money is used by the parties to a transaction as a medium of exchange. The benefit of using this currency, or more particularly cryptocurrency, is that no government interference is needed. IoT has several importance for a range of problems, however there are certain obstacles to be cleared [9].

E. Blockchain in IoT Payment Systems

Recent studies identify the IoT as a catalyst for seamlessly connecting physical and virtual objects, enabling the creation of novel digital services that enhance quality of life. However, the prevalent centralized architecture of IoT ecosystems introduces risks such as vulnerability to single points of failure, limited transparency, and weak data integrity. Blockchain technology including decentralized ledgers offers a promising alternative by distributing data across network nodes, thereby mitigating centralized risks and improving security, trust, and reliability within IoT networks [14].

In addition, due to impending improvements in blockchain technology, the instruments utilised to possibly handle the difficulties resulting from IoT. Blockchain offers greater levels of security and anonymity because it creates a secure computer environment using complicated cryptographic algorithms, hash functions, and timestamps. By mandating that the majority of contributing users

authenticate every data alteration, the blockchain also creates a tamper-proof and immutable record to safeguard data against destructive assaults [5]. As a consequence, a reliable system is established in which only IoT-based payment systems that are actually involved in a transaction may approve or disapprove it in accordance with their agreement. Additionally, it has been discovered that IoT devices may record a variety of real-time data, including delicate information like routines, passwords, and personal details [15].

Since the collected data are kept in a single location and are totally under the authority of a centralized third-party server, data privacy may be at danger. It is therefore simpler to hack when everything is centralized. Security is a significant issue as well, because the IoT centralised design only uses one server and one location for all data processing and storage activities, as such it is at risk for a number of issues, among which is DoS assaults [5].

Recent studies have demonstrated that integrating blockchain technology into IoT ecosystems significantly enhances system security, reliability, and resilience. Thanks to its decentralized and immutable ledger design, blockchain allows IoT networks to authenticate devices, trace interactions securely, and eliminate single points of failure common vulnerabilities in centralized architectures. Furthermore, blockchain's tamper-resistant structure ensures transparent and verifiable data integrity across interconnected devices, making it a powerful enabler for secure IoT deployment [16]. Blockchain accelerates peer-to-peer connections by utilizing the distributed ledger, as shown in Figure 1.

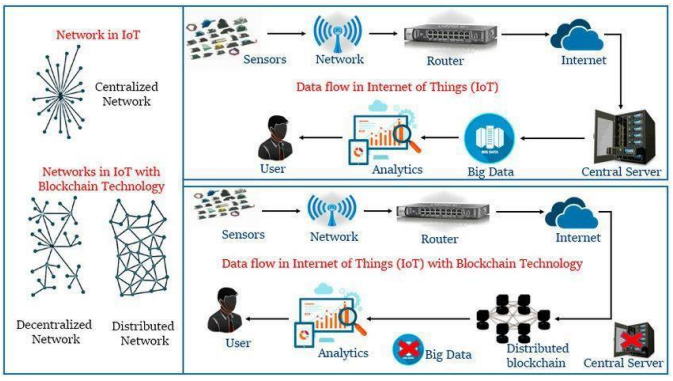

Figure 1: Blockchain technology and IoT [17]

The IoT data flow technique differs from utilizing just the IoT system when employing blockchain technology. The sources of data flow in the IoT with blockchain include the sensor, network, router, internet, distributed blockchain, and user. In this case, the distributed ledger is impenetrable and guards against incorrect data interpretation or authentication. Blockchain makes it more difficult to eliminate single thread communication (STC) in the IoT, which lowers system confidence. Blockchain use in IoT will improve the security, scalability and reliability of data flow [18].

Recent research underscores how private (permissioned) blockchains offer substantial benefits for financial institutions, notably in enhancing transactional security and operational efficiency. These systems enable controlled access, streamlined consensus mechanisms, and customizable governance resulting in significantly faster transaction times, reduced reliance on intermediaries, and lower labour and back-office costs. As such, private blockchains empower financial institutions to diversify their product offerings, generate new revenue streams, and deliver higher quality services to both existing and new customers [19].

Standardizing banking and financial sector solutions may greatly increase transaction speed and security, reduce labour costs and back-end expenditures, and remove transaction friction by utilizing private blockchain. As a result, the financial services industry will be able to increase the scope of goods and services it provides, create new sources of income, and improve the standard of care it provides to both present and new customers. In contrast to the publicly known public blockchains like bitcoin, private blockchains give users more control over the rules governing the network. They also allow users to be authorized before being allowed to participate (which is also known as permissioned blockchains) and may require participant identification. Private blockchains function by limiting network access via specific permission rules. Participants in the blockchain are restricted by certain access rules, which also restrict who may view network data, make contributions to the network, and be aware of transactions that occur on the network. Private blockchains enable more control over the network by restricting its participants, as access to particular features may require consenting to legally binding restrictions [20].

Private blockchain solutions can reduce costs and enhance efficiency by allowing peers to store data or encrypted versions of it on private ledgers that can be updated and refreshed with each new interaction and shared among authorized participants. These private blockchains strengthen data security within the network by implementing robust security protocols and access controls. Generally, blockchains allow participants to store and create an immutable, verifiable record of transactions necessary for processes like lending. Authorized users can then easily access these documents and records stored on or linked through the blockchain. By combining permanent record-keeping with stringent access controls, private blockchains support secure and efficient management of sensitive information related to financial transactions [21].

To address the limitations of IoT and Blockchain when used independently, this study proposes a hybrid framework that integrates the strengths of both technologies for secure and scalable payment systems. Figure 2 illustrates the conceptual model.

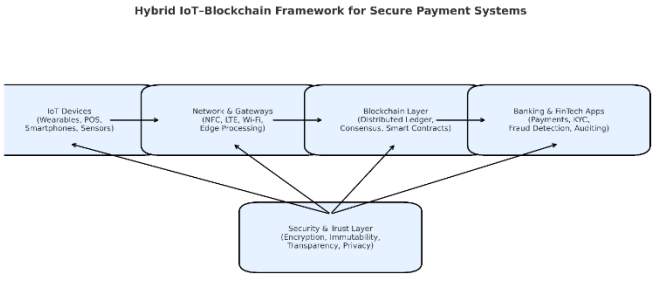

Figure 2: Hybrid IoT-Blockchain Conceptual Framework for Secure Payment Systems

Figure 2 illustrates the proposed hybrid IoT–Blockchain conceptual framework for digital payment systems, where IoT enables real-time transaction initiation and customer interaction, while Blockchain secures, validates, and records transactions in a decentralized and tamper-resistant manner.

The proposed conceptual framework integrates IoT devices with blockchain infrastructure to build a secure and efficient payment ecosystem. At the base, IoT devices such as wearables, mobile phones, and POS terminals initiate real-time payment requests, transmitting data through gateways and wireless networks. This data is encrypted and passed to the blockchain layer, where consensus mechanisms validate transactions and smart contracts automate processes like fraud detection and settlement. The validated transactions are stored in an immutable distributed ledger, ensuring transparency and trust. At the application level, banks, fintechs, merchants, and customers can access services including real-time payments, cross-border transfers, and automated auditing. By combining IoT's operational efficiency with blockchain's tamper-proof security, the framework enhances transaction integrity, scalability, and regulatory compliance while eliminating single points of failure.

F. Blockchain Consensus Algorithm

In a blockchain network, coming to a consensus is a big and difficult undertaking. Since every node in the network verifies a new block, new transaction records are appended to the blockchain. It should be noted that blocks cannot be changed or removed once they have been confirmed. Blockchains' structure is intended to hold up in an unstable, trust less network with hostile users. Numerous techniques are created as consensus algorithms [22]. The evolution of blockchain indicates that the quantity of these algorithms is growing every day. Proof of Work, Proof of Stake, Delegated Proof of Stake, Proof of Authority, Proof of Burn, Hybrid PoW/PoS consensus, Byzantine Fault Tolerance, Direct Acyclic Graph, Proof of Capacity, Proof of Identity, Tendermint, Round Robin, Proof of Elapse Time, etc. are a few examples of consensus algorithm types [23].

The Proof of Authority (PoA) algorithm, which is basically an improved equity proof model, was introduced by Wood 2017 [24]. PoA consensus differs from PoS consensus in that it uses the user's identification rather than their digital assets. Accordingly, it is predicated on the standing of reliable participants in a blockchain network [25]. The network verifies transactions and adds new blocks by relying on a number of pre-approved validators known as "authorities." Users who wish to be considered "authorities" must voluntarily reveal their identities, as the PoA algorithm stake's identity. Validators are required to adhere to a set of standards in order to be trusted. One of them requires people to register in the public notary database using the same identity they use on the site. For the network to work, more regulations have to be adhered to. Being a validator is a difficult job. During the screening process, candidates are required to demonstrate their long-term dedication to the network. Aside from financial commitment, they should be prepared to jeopardize their reputation in the selecting process. Finally, in order to guarantee that every applicant has an equal chance of obtaining the desired position, the process for choosing authorities must adhere to predetermined standards [26]. In return for identifying themselves and demonstrating their identity with official government documentation, validators are rewarded with authority and benefits.

G. Comparative Evaluation of Consensus Mechanisms

While the proposed framework adopts PoA for consensus, it is essential to situate this choice within the broader landscape of consensus algorithms. Table 1 presents a comparative overview of PoA, Proof of Stake (PoS), and Practical Byzantine Fault Tolerance (PBFT) in the context of digital banking applications.

Table 1: Comparative overview of PoA, PoS, PBFT

Consensus Mechanism	**Strengths**	**Weaknesses**	**Suitability for IoT-Banking**
PoA	Lightweight, fast validation, low computational demand; ideal for permissioned systems like banking	Requires trusted validators, may raise concerns over centralization	Highly suitable for IoT-enabled banking in Nigeria due to low resource demand and real-time validation
PoS	Energy-efficient, decentralized, resistant to certain attacks	Requires significant stake, validator selection can be biased, implementation complexity	Promising for future integration but less practical for current Nigerian financial infrastructures
PBFT	Fault-tolerant, high security, ensures transaction finality	Limited scalability with many nodes, communication overhead	Suitable for high-security scenarios but less efficient for large-scale IoT banking networks

This comparison highlights that PoA is the most practical choice for the Nigerian digital banking context, where efficiency, low resource consumption, and real-time settlement are critical. However, PoS and PBFT offer alternative pathways for future research. PoS, in particular, may be explored for cross-border payment systems where energy efficiency and scalability are paramount, while PBFT could enhance security in high-risk financial transactions.

The inclusion of this comparative perspective strengthens the contribution of this study by positioning PoA not merely as an isolated implementation but as a deliberate, context-sensitive choice within a spectrum of possible consensus mechanisms. In addition, to further justify the choice of consensus mechanism, a comparative evaluation of PoA, PoS, and PBFT was conducted. These mechanisms were assessed against four critical criteria for digital banking applications: scalability, security, energy efficiency, and suitability for IoT-enabled environments. Figure 3 presents the radar chart summarizing their relative performance.

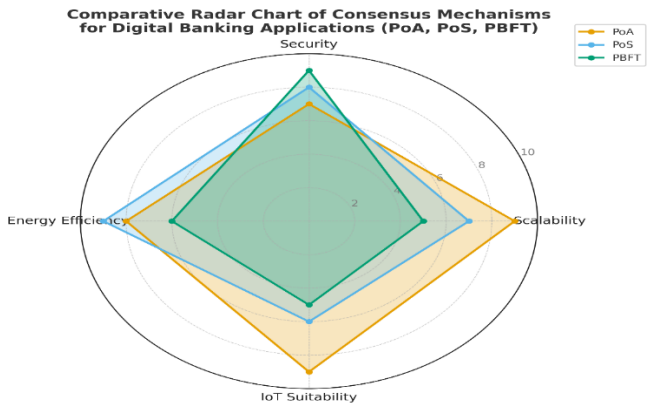

Fig 3: Comparative Radar Chart

The chart illustrates that PoA demonstrates high scalability, strong energy efficiency, and excellent suitability for IoT-based banking systems, though it offers slightly lower security compared to PBFT. PoS performs well in security and energy efficiency but is less optimized for IoT deployment in resource-constrained environments. PBFT ranks highest in security but lags in scalability and IoT suitability due to high communication overhead. Overall, the evaluation confirms that PoA is the most balanced and practical consensus mechanism for Nigeria's digital banking ecosystem, while PoS and PBFT remain promising alternatives for future integration in cross-border or high-security scenarios.

III. METHODOLOGY

This study adopts a theoretical and conceptual design approach to develop a hybrid Blockchain–IoT framework for secure digital payment systems. The methodology focuses on identifying the functional gaps in existing IoT-based financial infrastructures and integrating blockchain properties that effectively address these limitations.

A. Design Rationale

The design follows a multi-layer architecture composed of IoT device, network, and blockchain layers. Each layer performs a distinct role:

1. The IoT layer captures real-time transaction and user data.
2. The network layer handles encrypted communication and data transmission between devices and blockchain nodes.
3. The blockchain layer secures, validates, and records transactions using permissioned consensus protocols such as Proof of Authority (PoA).

This architecture was selected based on its potential to achieve scalability, low latency, and regulatory compliance which are key requirements for financial payment systems.

B. Assumptions

The proposed framework assumes that:

1. Participating IoT devices possess sufficient computational capability to execute lightweight blockchain functions (e.g., transaction signing).
2. Network connectivity between IoT nodes and blockchain validators is stable and bandwidth-efficient.
3. Authorized participants in the permissioned blockchain adhere to governance and compliance standards consistent with financial institutions.
4. The framework is implemented within a private or consortium blockchain to ensure data privacy and controlled access.

C. Limitations

As a conceptual design, the framework has not been empirically implemented or stress-tested under real-world transaction volumes. Scalability metrics, latency performance, and energy efficiency are inferred from existing literature rather than experimental data. Future work should include simulation, prototype development, and empirical validation to measure performance under varying transaction loads and network conditions.

IV. DISCUSSION

This study highlights the transformative potential of blockchain integration within IoT-driven financial ecosystems. Traditional IoT payment systems, though capable of real-time transaction processing, are inherently vulnerable due to their centralized architecture. Central servers create single points of failure, leading to risks such as cyberattacks, data breaches, and system downtime. By introducing blockchain's decentralization, immutability, and transparency, the proposed hybrid framework strengthens the trust and reliability of IoT-based payment infrastructures.

The use of permissioned (private) blockchains is particularly advantageous in financial applications where regulatory compliance, controlled access, and transaction speed are essential. Proof of Authority (PoA**)** enable rapid transaction validation without the high energy or computational demands typical of public blockchains. This enhances efficiency and scalability, ensuring that IoT payments can be processed securely and in real time. Furthermore, the integration of smart contracts automates payment execution, fraud detection, and settlement verification which are functions that reduce reliance on intermediaries and improve operational transparency.

From a theoretical standpoint, the proposed hybrid framework demonstrates strong alignment with emerging financial technology trends emphasizing **s**ecurity by design, distributed trust, and regulatory adaptability. By combining IoT's dynamic data acquisition with blockchain's tamper-proof transaction management, the framework advances a model suitable for next-generation digital banking and automated financial services.

However, practical deployment in real-world environments faces several technical and regulatory constraints. Data regulation especially under frameworks such as the EU's GDPR or Nigeria's NDPR requires that personal financial data remain identifiable yet protected within distributed systems. Balancing blockchain's transparency with compliance-oriented data privacy remains a complex task. Similarly, hardware limitations among IoT devices can restrict the computational ability to support blockchain operations such as cryptographic hashing or local validation, particularly in low-power or edge devices. Scalability trade-offs also persist: increasing decentralization enhances security but can introduce higher latency

and bandwidth demand during transaction synchronization across nodes.

In addition, potential implementation challenges must be critically considered. Latency remains a major concern when validating transactions across multiple nodes, especially in time-sensitive financial operations. Interoperability between heterogeneous IoT devices and different blockchain platforms presents another obstacle, as standardized communication protocols are still under development. Moreover, deployment costs including infrastructure setup, node maintenance, and energy consumption may limit adoption among smaller financial institutions or in developing regions. These factors highlight the need for pilot testing, modular scalability, and energy-efficient consensus designs before full-scale implementation.

Overall, the findings indicate that blockchain-enabled IoT payment systems can significantly enhance the security, transparency, and efficiency of digital financial services. Yet, successful implementation will depend on addressing real-world constraints through adaptive regulatory frameworks, lightweight technical designs, and strategic cost management. Future research should explore empirical validation, cross-chain interoperability solutions, and sustainable deployment models to ensure that blockchain–IoT integration achieves both technological robustness and socio-economic feasibility.

V. CONCLUSION AND SUGGESTION FOR FUTURE STUDIES

This paper contributes a hybrid Blockchain–IoT framework specifically designed to enhance the security, efficiency, and regulatory compliance of digital payment systems. Unlike existing IoT models that rely on centralized data management, the proposed framework leverages blockchain's decentralization, immutability, and smart contract automation to eliminate single points of failure and reduce reliance on third-party intermediaries. By integrating permissioned blockchain architecture with IoT networks, this study advances a scalable and tamper-resistant model suitable for real-time financial transactions in both developed and developing contexts.

The findings demonstrate that combining IoT's real-time connectivity with blockchain's distributed security mechanisms can significantly strengthen transaction integrity, data privacy, and operational efficiency. The framework supports secure peer-to-peer payments, automated auditing, and regulatory transparency, making it a viable foundation for future digital banking ecosystems.

While the study presents a conceptual design, it lays essential groundwork for practical implementation by identifying key challenges such as latency, interoperability, and compliance that must be addressed in subsequent research. Future studies should therefore focus on:

1. Prototype Development and Testing: Implement and evaluate the framework in real-world financial settings to assess performance and scalability under varying transaction volumes.
2. Cross-Chain Interoperability: Develop mechanisms to enable communication between different blockchain networks for seamless cross-border payments.
3. Regulatory and Compliance Models: Examine how blockchain-enabled IoT payment systems align with financial regulations and data protection laws.
4. Energy Efficiency and Sustainability: Explore consensus algorithms that minimize resource consumption while maintaining high throughput and security.
5. User Adoption and Behavioural Analysis: Investigate factors influencing customer trust and willingness to engage with blockchain-based IoT financial systems.

In summary, this study provides a theoretical and architectural foundation for secure, scalable, and compliant IoT-based payment systems. By bridging blockchain innovation with IoT infrastructure, it offers a pathway toward next-generation digital finance that is resilient, transparent, and adaptable to global financial transformation.

REFERENCES:

[1] M. Sober, M. Sigwart, P. Frauenthaler, C. Spanring, M. Kobelt, and S. Schulte, "Decentralized cross-blockchain asset transfers with transfer confirmation," *Cluster Computing*, vol. 26, pp. 2129–2146, 2022

[2] Z. Hussein, M. A. Salama, and S. A. El-Rahman, "Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms," *Cybersecurity*, vol. 6, no. 1, p. 30, 2023.

[3] H. Adam, "Blockchain Facts: What It Is, How It Works and How It Can Be Used," 2023. [Online]. Available: https://www.investopedia.com/terms/b/blockchain.asp. [Accessed: Sep. 16, 2025].

[4] V. Gabriel, "Blockchain technologies could boost the global economy USD 176 trillion by 2030," PwC, 2023. [Online]. Available: https://www.pwc.ro/en/press-room/press-release-2020/PWC

[5] S. Ahamad, P. Gupta, P. A. Bikash, K. K. Padma, Z. Khan, and M. F. Hasan, "The role of blockchain technology and Internet of Things (IoT) to protect financial transactions in cryptocurrency market," *Materials Today: Proceedings*, vol. 56, no. 1, pp. 2070–2074, 2022.

[6] W. Liang and N. Ji, "Privacy challenges of IoT-based blockchain: a systematic review," *Cluster Computing*, vol. 25, no. 3, pp. 2203–2221, 2022.

[7] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed: Apr. 4, 2019].

[8] Hyperledger, *An introduction to Hyperledger*. The Linux Foundation, 2020. [Online]. Available: https://www.hyperledger.org/wpcontent/uploads/2020/08/Hyperledger_WhitepaperIntroduction.pdf. [Accessed: Sep. 16, 2025].

[9] J. Ali, T. Ali, S. Musa, and A. Zahrani, "Towards secure IoT communication with smart contracts in a blockchain infrastructure," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 11031–11044, 2020.

[10] Y. Sharma, B. Balamurugan, N. Snegar, and A. Ilavendhan, "How IoT, AI, and Blockchain will revolutionize business," in

Blockchain, Internet of Things, and Artificial Intelligence, 2021, p. 235.

[11] P. Garg, B. Gupta, A. K. Chauhan, U. Sivarajah, S. Gupta, and S. Modgil, "Measuring the perceived benefits of implementing blockchain technology in the banking sector," *Technological Forecasting and Social Change*, vol. 163, p. 120407, 2021.

[12] B. Ademola, "Cryptocurrency Trading: CBN Orders Banks to Close Operating Accounts," 2023. [Online]. Available: https://www.cbn.gov.ng. [Accessed: Sep. 16, 2025].

[13] S. K. Dwivedi, P. Roy, C. Karda, S. Agrawal, and R. Amin, "Blockchain-based internet of things and industrial IoT: a comprehensive survey," *Security and Communication Networks*, vol. 2021, no. 1, p. 7142048, 2021.

[14] H. D. Dhiai, P. Varga, and S. Molnár, "Leveraging blockchain technology for ensuring security and privacy aspects in Internet of Things: A systematic literature review," *Sensors*, vol. 23, no. 2, p. 788, 2023.

[15] M. Pashkevych, L. Bondarenko, A. Makurin, I. Saukh, and O. Toporkova, "Blockchain technology as an organisation of accounting and management in a modern enterprise," *International Journal of Management*, vol. 11, no. 6, pp. 229–235, 2020.

[16] G. B. Naidu, "Blockchain technology as a security enhancement framework for Internet of Things: A comprehensive analysis," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 2024. doi: 10.32628/CSEIT241061121.

[17] N. M. Kumar and P. K. Mallick, "Blockchain technology for security issues and challenges in IoT," *Procedia Computer Science*, vol. 132, pp. 1815–1823, 2018.

[18] B. Li, R. S. Chen, and H. Wang, "Using intelligent prediction machine and dynamic workflow for banking customer satisfaction in IoT environment," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–10, 2021.

[19] P. Munglani, S. Riaño, and K. Karlapalem, "Performance evaluation of permissioned blockchains for financial applications: The ConsenSys Quorum case study," *Blockchain: Research and Applications*, vol. 3, no. 1, p. 100026, 2021, doi: 10.1016/j.bcra.2021.100026.

[20] S. M. Varma and S. T. Maguluri, "Throughput optimal routing in blockchain-based payment systems (codes)," 2020. [Online]. Available: https://github.com/gt-coar/BlockchainP2P. [Accessed: Sep. 16, 2025].

[21] M. R. Kabir and M. A. Islam, "Behavioural intention to adopt blockchain technology in Bangladeshi banking companies," in *AIP Conference Proceedings*, 2021, pp. 23–47.