Research Paper

Security capabilities of blockchain technology on iot-based payment system

Maimunatu Ya'u Ibrahim[1*], Kabiru Ibrahim Musa[2], Aminu Ahmad[3]
[1*,2,3]Department of Management and Information Technology, Abubakar Tafawa Balewa University Bauchi, Nigeria.

Article Info

Article History:
Received: 18 October 2025
Revised: 30 December 2025
Accepted: 06 January 2026
Published: 20 February 2026

Keywords:
IoT
Blockchain
Security Payment System
Digital Banking

ABSTRACT

This study examines at how blockchain can improve the security of digital banking systems based on the Internet of Things. These systems are vulnerable because of their centralized structures and limited device capability. 404 bank account holders with IT and blockchain expertise participated in the poll, which evaluated their opinions on how well blockchain works to improve data security, integrity, and traceability. The findings show that there is broad consensus that blockchain improves security and trust by enabling decentralization, encryption, and unchangeable records. The study concluded that using blockchain technology is essential for designing scalable and secure digital payment systems in dynamic marketplaces.

Corresponding Author:
Maimunatu Ya'u Ibrahim
Department of management and Information Technology, Abubakar Tafawa Balewa University Bauchi, Nigeria.
Email: yimaimunatu.pg@atbu.edu.ng

1. INTRODUCTION

The rapid expansion of the Internet of Things (IoT) has changed the way objects communicate and interact, resulting in the development of intelligent, networked environments that support anything from financial services to smart homes. IoT-based payment solutions, in particular, are becoming widely accepted because to their potential to facilitate seamless, immediate transactions over unified devices [1].

However, this incorporation also presents thoughtful security alarms. IoT devices usually work with restricted computing resources, absence of vigorous security mechanisms, and are frequently employed in unsafe environments, making them susceptible to cyber threats such as data interception, spoofing, and unauthorized access. Conventional security architectures developed around centralized control systems are progressively insufficient in tackling these vulnerabilities. Centralized systems undergo single points of failure, controlled scalability, and inadequate transparency, which expose IoT payment networks to systemic threats. These restrictions require state-of-the-art methods that offer distributed control, immutable record-keeping, and secure peer-to-peer contact through resource constrained devices [2].

Blockchain technology has emerged as a transformative way out with the prospective to boost the security of IoT-based payment systems. Its main features comprising decentralization, cryptographic hashing, and consensus mechanism which ore means for securing transactions and upholding trust without centralized mediators. Additionally, payment transactions can be virtually executed because of smart contracts, which guarantee transparency while minimizing operational costs and cyber-attacks risks [3]. Regardless of these advantages, it is still difficult to incorporate blockchain technology with IoT. Instantaneous execution in payment systems is troubled by hurdles such elevated energy and processing needs, delay problems, and constrained interoperability with lightweight IoT protocols [1], [2]. Discovering improved blockchain technologies that are compatible with IoT systems' limitations is therefore very important. This paper looks at the security potential of blockchain technology in IoT-based payment systems. The paper analyzes the security areas where blockchain can emerge as a solution, such as resilience against endeavours to disrupt through hacking, keeping data private, ensuring that the data is secure and accurate, and issuing permissions. The result is to offer insight on the growth of additional secure, scalable, and efficient digital payment bases created for the growth of IoT ecosystem [2].

IoT device incorporation into digital banking and payment systems has brought about substantial security weaknesses in addition to different levels of proficiency and connectivity. These restrictions stem from the IoT technology limitations which includes among others insecure communication methods, low processing capability and poor encryption. The resulting problems of such weak points are loss of funds, identity theft and user trust being eroded in the case of financial transactions where the safety of transactions and data integrity are very important [2]. Centralized security models have thus shown to be insufficient for the dispersed and extended nature of IoT systems due to their centralized vulnerabilities and ineffectiveness in the face of distributed attacks [1]. A scalable, secure, and transparent way of transaction management and authentication is more important than ever, as digital financial services are becoming more and more reliant on connected devices.

Blockchain technology is seen as the eco-friendly way out due to its distributed structure, cryptographic authentication, and non-repudiation of transactions in the form of ledgers. However, its widespread application in IoT payment systems would still be restrained by the high computational requirements, latency problems, and energy consumption that clash with the lightweight and resource-limited IoT devices' design [2], [3]. Although prior research has emphasized blockchain's theoretical advantages, empirical evaluations specifically addressing its capacity to resolve IoT-related security threats in the payment domain are scarce. This study seeks to examine the degree to which security capabilities of blockchain can provide a real-world and efficient security framework for IoT-based payment systems, especially in ensuring privacy, data integrity, and resilience under controlled conditions. The results will add to the current discourse on making protected, scalable digital financial environment.

2. RELATED WORK

Table 1. Table of Related Empirical Studies on Iot and Blockchain

References	Research Area	Methodology/ Algorithm Used	Findings	Future Scope

[4]	Digital Payment Trust	Large-scale quantitative survey (540 respondents)	Blockchain mediates trust, reduces risk, enhances usability	Explore longitudinal impacts of blockchain trust over time
[5]	IoT Security Threat Mapping	Systematic textual analysis	Mitigates spoofing, tampering, and availability threats	Apply threat-mapping model in real-time scenarios
[6]	Blockchain integration in embedded IoT systems	Comparative and analytical synthesis of existing blockchain-IoT solutions	Blockchain enhances security, data integrity, trust, and decentralization in embedded IoT systems	Development of lightweight and energy-efficient blockchain architectures
[7]	Edge-IoT Payments	Prototype evaluation of EdgeChain	Enhanced auditability, latency suitable for real-time apps	Deploy and test in live IoT payment networks
[8]	Blockchain-Based IoT System	Permissioned blockchain with a delegated trust model	Improved scalability and reduced transaction latency compared to traditional blockchain approaches	Support dynamic trust management
[9]	Blockchain-enabled distributed learning for consumer IoT	Blockchain-based distributed learning framework	Significant scalability improvements and Enhanced data security, trust, and privacy	Advanced consensus mechanisms
[10]	Secure Event Logging	Blockchain-backed logging evaluation	High throughput, tamper resistance for payment logs	Adapt to financial transaction auditing
[11]	Blockchain scalability in low-powered IoT sensor networks	Simulation-based experimental evaluation	Rise in latency, energy consumption, and network congestion	Lightweight blockchain architectures
[12]	IoT Data Management	DPoS + IPFS blockchain framework	≤0.976 ms latency and high throughput	Deploy for ultra-fast IoT micro-payments
[13]	IoT-based Payment via Smartphone	Bluetooth and smartphone relay	Limited to micro-payments; Bluetooth security weak	Improve pairing methods and wearable tech integration
[14]	Industrial IoT Blockchain	Lightweight Layered Blockchain Framework (LLBF)	Improved throughput, reduced processing overhead	Apply to security-sensitive factory settings
[15]	Scalable IoT Payments	Multi-layer permissioned blockchain + IPFS + Bloom filters	Reduced latency to 1.21s (0.025s cached), high responsiveness	Deploy for national-scale IoT payment ecosystems

[16]	Anonymous Payments	Conditional anonymity blockchain protocol	Traceable yet revocable anonymity in transactions	Implement lawful private payment systems
[17]	Blockchain Use in Korea's FinTech	Case study of 4 blockchain applications	Monitors settlement, remittance, smart contracts; lacks privacy focus	Investigate consumer confidentiality in consortium systems
[18]	Banking Cybersecurity	Security architecture model with blockchain + zero trust	Enhances breach prevention through continuous authentication	Apply model to national-level financial cybersecurity systems
[19]	Cloud-based E-Banking Security	Blockchain + Smart Contracts (empirical evaluation)	Improved trust, reduced tampering and insider fraud in e-banking	Deploy across large financial institutions
[20]	CBDC + Blockchain Payments	Hybrid permissioned blockchain + CBDC (performance benchmarking)	High throughput, low latency, secure digital currency settlements	Expand into cross-border payment networks
[21]	IoT Transaction Protocols	Comparative simulations with proxy re-encryption	Improved confidentiality and attack resilience	Integrate into commercial IoT payment systems

Table 1 Studies have shown that IoT security in IoT systems may be enhanced more successfully by leveraging blockchain technology. These tasks may be performed using blockchain technology, enabling IoT systems to track a large number of networked and linked devices. Blockchain enables IoT systems to conduct dealings with coordinated gadgets. Blockchain can improve the resilience, security, and dependability of IoT systems [22]. As illustrated in Figure 1, blockchain uses the distributed ledger to speed up peer-to-peer connections.

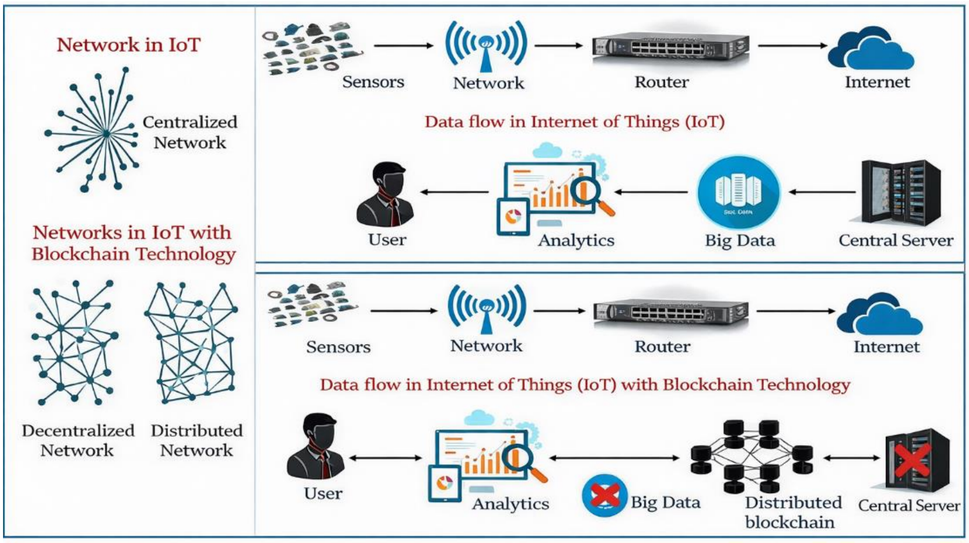

Figure 1. Blockchain Technology and Iot

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 [16], [22].

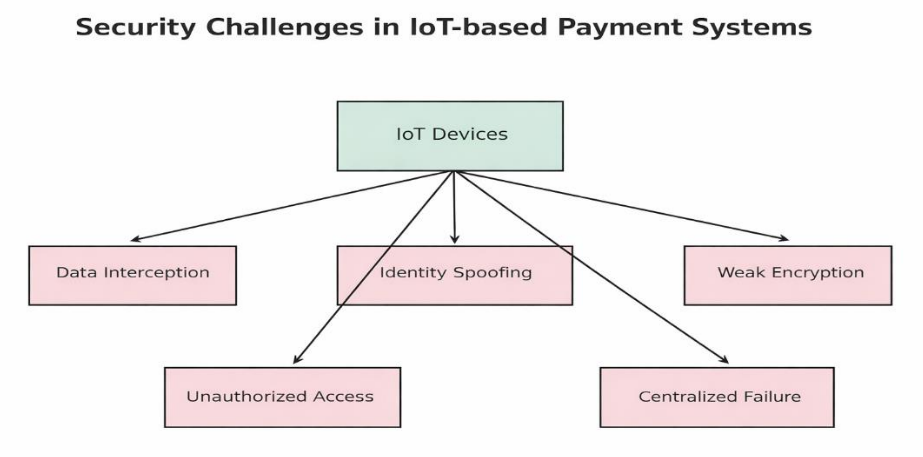

Figure 2. Security Challenges in IoT-based Payment Systems

Figure 2 displays the main security issues which IoT-based payment systems faces. These challenges are as a result of single point-point network topologies, fragile encryption measures, and controlled device size as illustrated in the Figure 2, the challenges like identity spoofing, data breach, and denial-of-service (DoS) attacks can reveal transaction consistency and user trust. This reinforces the idea that in order to reduce financial risks and improve transparency, distributed, robust solutions like blockchain are essential.

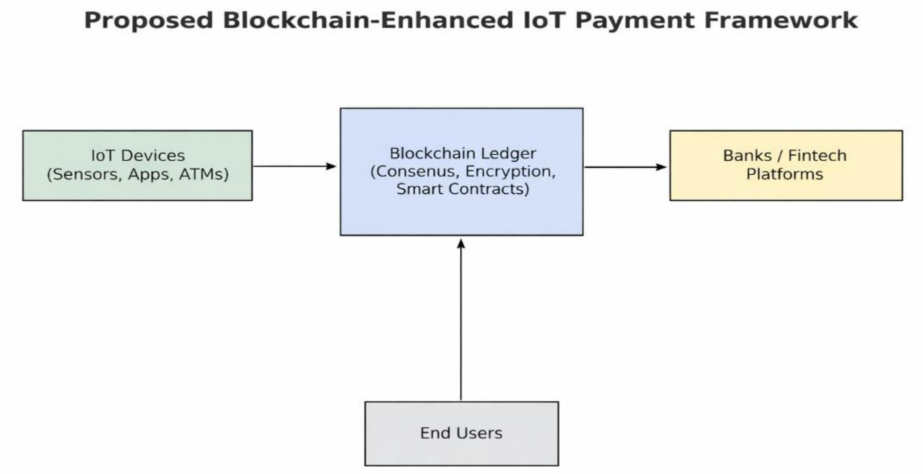

Figure 3. Proposed Blockchain-Enhanced IoT Payment Framework

The proposed blockchain-enhanced IoT payment framework is revealed by Figure 3. The framework comprises a decentralized blockchain ledger, protected by smart contracts and consensus methods, alongside IoT devices. This ensures decentralization, immutability, and auditability, thus mitigating the drawbacks of centralization. Moreover, improved traceability and fraud prevention are benefits to banks and fintech companies. Consequently, the framework proposes a reliable way for increasing IoT-driven financial services while protecting user information.

3. METHODOLOGY

This study adopts a descriptive survey which aligns with the research objective to evaluate user perception of blockchain in banking.

Commercials bank clients in Bauchi State metropolitan is the population of the study, the respondents are the banks customers from academic environments (Tertiary Institutions) and the goal of the study was to determine if Nigerian banking and fintech businesses will require a secure digital payment system. The entire commercial banks clients in Bauchi metropolitan made up the population of the study.

The Bauchi metropolitan area is home to 46 commercial banks, according to the Bauchi State Inland Revenue. There are 135million active bank accounts in Nigeria NIBSS (2023), whereas there is population of 670,280 in Bauchi metropolitan area (World Population Review, 2023). In light of that, the approximate percentage of the active account in Bauchi metropolitan area is 20,141 (135,000,000/670,280 x 100). Krejcie and Morgan 1970 Table for calculating sample size from a given population says a population of 20,000 people should have a sample size of 377 samples; as a result, the study's sample size is 377 respondents. The study employed cluster sampling to classify respondents, then within each cluster, purposive sampling was employed to pick respondents with expert knowledge.

Data was collected using questionnaire from 404 respondents who are from academic environment because of their knowledge of blockchain technology. Two sections made up the questionnaire, which was adapted from Khalilzadeh (2017): While Section B evaluated the security potential of blockchain technology in augmenting IoT-based payment systems, Section A collected demographic data. Responses were measured using a five-point Likert scale ranging from strongly disagree to strongly agree.

Given that the research methodology used for this study is a descriptive survey, the questionnaires that were gathered were split into two portions, A and B. Simple frequency and percentage was used to analyse the respondents' demographic data in Section A, and the software application's simple frequency and mean were used to analyse the data in Section B. The statistical package of social sciences research, or SPSS version 29, is a software program used for social science research methods. It is the tool that was utilized for data analysis in this study.

4. RESULTS AND DISCUSSION

The research was carried out on the specialized set of customers from commercial banks in Bauchi metropolitan area. A questionnaire survey instrument was shared and retrieved from the sample of 404 respondents across the Bauchi metropolitan area. After the data collection, the questionnaires were uploaded into SPSS software for analysis. This response rate is considered adequate for the study based on Krejci and Morgan (1970). The data was collected using google form, while the data was analysed using IBM-SPSS software version 29. The data was uploaded into SPSS application software, where the coded data were cleaned to check for errors and wrong entries. The data screening was done primarily in order to improve the quality of the data.

4.1. Demographic Variables

The research instrument has three demographic variables which are age range, digital banking usage, and digital banking frequent use. Table 2 show the detail result of the demographic variables obtained showing frequencies and percentages of each.

Table 2. Respondents Information

Demographics	Category	Frequency	Percentage
Age range	18-28yrs	229	56.7%
	29-39yrs	128	31.7%
	40-50yrs	36	8.9%
	Above 50	11	2.7%

	Total	404	100%
Digital Banking Usage	Less than 1yr	31	7.6%
	1-3yrs	82	20.3%
	Over 3yrs	291	72.0%
	Total	404	100%
Digital Banking Service Frequent Use	Every day	284	70.3%
	Once or twice a week	87	21.5%
	Rarely	33	8.2%
	Total	404	100%

Based on the result as shown in Table 2, 229 of the respondents fall between the age range of 18 and 28 years with 56.7% which is the highest and stands at, those between 29 and 39 years have a frequency of 128 with 31.7%; followed by those who fall between the range of 40 and 50 years with a frequency of 36 and a percentage of 8.9%; while those above 50 years were the least, representing 2.7% and with a frequency of 11. Analysing the result based on digital banking usage, those with less than a year of usage have a frequency of 31 and a percentage of 7.6%; those with 1-3 years have a frequency of 82 and a 20.3% and those with over 3 years have the highest frequency of 291 and a 72.0%. Regarding the question on the duration of frequent digital banking use, 284 respondents use digital banking every day, with a percentage of 70.3%, which is the highest, followed by those who use digital banking once or twice a week with a frequency of 87 and a percentage of 21.5, and lastly, those who rarely use digital banking have a frequency of 33 and a percentage of 8.2%. In light of the above, the result seems to show that those between the ages of 29 and 39 engage in one form of digital banking or another. It also shows that the respondents have been using digital banking for 1 to 3 years, and their frequent use is at least one a day. This research emphasises how digital banking is becoming more and more common, especially among younger users and those who have been using it for a while. It also implies that a lesser percentage of users use it less regularly, with the bulk of users indicating that daily usage is usual.

4.2. Descriptive Statistics of the Items

The Table 3 displays the detailed descriptive statistics of each item based on the responses obtained. The items were assessed using the 5-point Likert scale, which ranges from low to high and represents the degree of performance. There are five ranges on this scale: 1.00-1.80 for strongly disagree, 1.81-2.60 for disagree, 2.61-3.40 for undecided, 3.41-4.20 for agree and 4.21-5 for strongly agree.

Table 3. Scoring Range of Likert Scale of the Survey

Scale	Value	Range
Strongly Disagree	1	1.00 - 1.80
Disagree	2	1.81 - 2.60
Undecided	3	2.61- 3.40
Agree	4	3.41 - 4.20
Strongly Agree	5	4.21 - 5.00

Table 4. Security Capabilities of Blockchain on the Performance of the Existing Payment System

S/n	Questionnaire Items	SD(1)	D(2)	U(3)	A(4)	SA(5)	Mean	St.D
1	I would feel totally safe providing sensitive information about myself when using a blockchain-based digital banking payment system.	23 5.7%	28 6.9%	89 22.0%	169 41.8%	95 23.5%	3.71	1.01
2	I believe that blockchain-based digital banking payment offer significant advantages over	25 6.2%	13 3.2%	37 9.2%	185 45.8%	144 35.6%	4.01	0.78

	traditional banking payment systems.							
3	Blockchain-based digital banking payment systems does not cause financial risk.	23 5.7%	84 20.8%	106 26.2%	146 36.1%	45 11.1%	3.26	1.20
4	I am likely to recommend a blockchain-based digital banking platform to others based on its security features and benefits.	22 5.4%	25 6.2%	58 14.4%	203 50.2%	96 23.8%	3.81	1.14
5	Blockchain-based digital banking payment system has sufficient security capabilities to ensure user's information cannot be modified by hackers.	17 4.2%	29 7.2%	74 18.3%	186 46.0%	98 24.3%	3.79	1.04
6	Blockchain-based digital banking payment systems abides by personal data protection law.	16 4.0%	14 3.5%	65 16.1%	219 54.2%	90 22.3%	3.87	1.18
7	Blockchain technology will provide a safe digital banking payment system for banks and fintech industries.	11 2.7%	8 2.0%	45 11.1%	228 58.4%	112 27.7%	4.04	0.76
8	Blockchain technology will ensure complete financial transaction security.	11 2.7%	14 3.5%	45 11.1%	204 50.5%	130 32.2%	4.06	0.72
9	Financial transaction traceability issues and security flaws will be addressed with the help of blockchain technology.	15 3.7%	20 5.0%	59 14.6%	203 50.2%	107 26.5%	3.91	0.88
10	Blockchain technology will make it possible for systems to function independently, without a central authority by doing away with intermediaries.	13 3.2%	24 5.9%	54 13.4%	184 45.5%	129 31.9%	3.97	0.92
	Overall Mean Score						3.84	0.96

Table 4 shows how the security aspects of blockchain technology affect how the current IoT-based payment system operates. According to the respondents' responses, item 8, which claims that blockchain technology would ensure end-to-end security for financial operations, has the greatest mean (4.06) and standard deviation (0.72). Item 7, which claims that blockchain technology will provide a safe digital banking payment system for banks and fintech industries, came in second, with a 4.04 mean and a standard deviation of 0.76.

Item 2 (I believe that blockchain-based digital banking payment offer significant advantages over traditional banking payment systems) and item 10 (which claims blockchain technology will make it possible for systems to function independently, without a central authority by doing away with) have mean scores of 4.01 and 3.97, and a standard deviation of 0.78 and 0.92 respectively. Item 9 claimed that Blockchain technology will assist in addressing security vulnerabilities and traceability problems in financial transactions has a mean score of 3.91 and a standard deviation of 0.88.

Additionally, item 6 (which has a mean score of 3.87 and a standard deviation of 1.18) said that Blockchain-based digital banking payment systems abides by personal data protection law. Item 4 (which has a mean score of 3.81and a standard deviation of 1.14) stated that I am likely to recommend a blockchain-based digital banking platform to others based on its security features and benefits. Item 5, which claimed that Blockchain-based digital banking payment system has sufficient security capabilities to ensure user's information cannot be modified by hackers, gets a mean score of 3.79 and a standard deviation of 1.04.

The lowest mean score goes to Item 3 with 3.26 and the highest standard deviation of 1.20 stated that Blockchain-based digital banking payment systems does not cause financial risk. Followed by Item 1, which stated that (I would feel totally safe providing sensitive information about myself when using a blockchain-based digital banking payment system) with the mean score of 3.71 and a standard deviation of 1.01. Essentially, the range of 3.41 to 4.20 denotes "agree," according to the criterion mentioned above. Consequently, the findings demonstrate that most respondents agreed with the purpose as stated in the table, with an overall mean score of 3.84 and average standard of deviation of 0.96.

It is imperative to note that the purpose of the questionnaire was to investigate how blockchain technology's security capabilities affected the functioning of the existing IoT system, which this research aims to enhance by developing a blockchain-based digital banking payment system. According to published research, blockchain technology has certain advantages such immutability, which makes data entered into the ledger unchangeable, and it makes asset monitoring and transaction recording easier. Transparency (making changes to blockchains available to all entities for analysis and access), reliability (reducing the risk of a single point of failure and boosting resistance against attacks), and integrity (transactions to be carried out precisely as instructed by the protocol) are three more blockchain technology capabilities that can enhance the existing IoT-based system. It could be likely to increase all of these features in transactions, which would enhance safety and save a lot of money [23].

The main advantage of blockchain technology is that it would eradicate intermediaries, aside its numerous other advantages. Consequently, the existing IoT-based system will no longer need a middleman thanks to the proposed study methodology. Furthermore, the survey's results indicate that, in comparison to the present IoT-based framework, the payment system's security will be enhanced by blockchain technology. In a similar vein, blockchain encourages transparency by letting users track and view past network transactions. As such, it can be trusted to identify the source of any data leaks and apply urgent remedies. Similarly, IoT use is expanding, but there are worries about security, privacy, safety, and scalability. Blockchain was first developed to manage cryptocurrencies, but it has been used with IoT to enhance it because to its decentralized structure and enhanced safety, integrity, security, and privacy. Because blockchain's "security by design" feature can assist address significant security challenges in IoT-based systems, a blockchain-based digital banking payment system is required [24]. Lastly, the outcomes of the study's main aim will be used as a contribution to develop a blockchain-based digital banking payment system, with blockchain technology being the first criterion.

4.3. Discussion

After the conclusion of the descriptive statistics analysis for the questionnaire items, the research objective was achieved. The study highlights the strong security properties of blockchain technology and how it may enhance IoT-based payment systems. Respondents generally agreed that blockchain enhances digital banking security through immutability, decentralization, and cryptographic security, with an overall mean score of 3.84 and a standard deviation of 0.96. These features assisted in minimizing security threats like scam, illegal access, and data modification. The findings agree with previous studies, such as [25], which indicated that blockchain technology enhances the security of electronic payments, the transparency of transactions, and the effectiveness of payments. The participants in the survey pointed out that one of the major advantages of blockchain technology is the end-to-end security it can provide for financial transactions. They also emphasized its potential to revolutionize financial services by removing middlemen and thereby lowering costs (the average score was 4.06).

Moreover, the present research also indicates that it could be the case for digital financial transactions that blockchain is the factor of the increased transparency and trust. With the use of distributed ledger technology and consensus mechanisms, blockchain guarantees secure and unchangeable transaction records, which in turn allows immediate evaluations and leads to a decrease in fraudulent activities. This concurs with [24], which illustrated how blockchain is an important factor in building trust and credibility in online banking. Respondents acknowledged that blockchain's security mechanisms significantly improve transparency and credibility within financial transactions, making it a valuable addition to existing payment systems.

4.4. Summary of Findings

The security, speed, and transparency of digital banking payment systems are significantly enhanced by the use of blockchain as shown in this study. According to the mean score of 3.84 from the descriptive statistics, the respondents are of the opinion that blockchain's security features, such as cryptographic hashing, and decentralization, would have an enormous positive impact on the working of the IoT-based payment systems. These results are in agreement with a prior study by [25] that shows how blockchain has a significant effect on electronic payment systems, enhancing the availability of financial services by improving security and payment speed and minimizing the need for intermediary.

5. CONCLUSION

This study examined how blockchain technology could strengthen the security of IoT-based digital payment systems. The study asserts that blockchain's decentralization, immutability, and end-to-end encryption tackle major weaknesses in the existing centralized payment systems. The people who answered the survey were in general agreement about the improvement of transaction visibility, data integrity, privacy, and trust by blockchain, especially, the ones with IT and blockchain expertise. Also, Blockchain enhances the digital finance climate in terms of both scalability and operational efficiency by removing middlemen and allowing secure peer-to-peer communication. To put it differently, the adoption of blockchain technology in the IoT-centric financial sector is not only necessary but also very feasible if we are to have robust and secure payment systems.

Acknowledgement

Author is very grateful for the support and cooperation of the management and staff of the participating commercial banks in Bauchi State, Nigeria, who were very generous with their time and very willing to participate in this study. We would especially like to thank the instructors and students from the computer science and information technology departments at the chosen postsecondary institutions for their knowledgeable contributions. The author also extends gratitude to academic mentors and colleagues whose insights and constructive feedback greatly enriched the quality of this research.

Funding Information

The authors declare that no funds, grants, or other forms of financial support were received for the preparation or publication of this manuscript.

Author Contributions Statement

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Maimunatu Ya'u Ibrahim	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓		✓	
Kabiru Ibrahim Musa	✓	✓		✓				✓		✓		✓		
Aminu Ahmad	✓	✓		✓				✓		✓		✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal Analysis

I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting

Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject Administration
Fu : **Fu**nding Acquisition

Conflict of Interest Statement

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper. Authors state no conflict of interest.

Informed Consent

All participants were fully informed about the purpose, scope, and nature of the study before data collection. They received assurances that their involvement was completely optional and that they may leave at any time without incurring any fees. Prior to completing the questionnaire, informed consent was acquired, and participants were assured of their identity and confidentiality. The comments were utilized only for academic purposes, and no personally identifiable information was gathered.

Ethical Approval

This study was carried out in compliance with Abubakar Tafawa Balewa University's ethical guidelines in Bauchi, Nigeria. The Departmental Research Ethics Committee examined and approved the research protocol, which included the survey instrument and consent procedures.

Data Availability

The data that support the findings of this study are available from the corresponding author, M.Y.I., upon reasonable request.

REFERENCES

[1] L.-H. Wang, Z. Pan, H. Jiang, H.-L. Lai, Q.-P. Ran, and P. A. R. Abu, 'A low-power passive UHF tag with high-precision temperature sensor for human body application', IEEE Access, vol. 10, pp. 77068-77080, 2022. doi.org/10.1109/ACCESS.2022.3193155

[2] L. Rodić, T. Perković, M. Škiljo, and P. Šolić, 'Privacy leakage of LoRaWAN smart parking occupancy sensors', Future Gener. Comput. Syst, vol. 138, pp. 142-159, Jan. 2023.doi.org/10.1016/j.future.2022.08.007

[3] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, 'On Blockchain and its integration with IoT', Future Gener. Comput. Syst, vol. 88, pp. 173-190, 2018.doi.org/10.1016/j.future.2018.05.046

[4] V. Pandey and G. S. Kushwaha, 'From risk minimisation to trust building: An empirical study on blockchain technology in digital payment system', J. Modelling Manag.

[5] M. El-Masri and E. M. A. Hussain, 'Blockchain as a mean to secure Internet of Things ecosystems - a systematic literature review', J. Enterp. Inf. Manag, vol. 34, no. 5, pp. 1371-1405, Nov. 2021.doi.org/10.1108/JEIM-12-2020-0533

[6] M. Darbandi, H. M. R. Al-Khafaji, S. H. Hosseini Nasab, A. Q. M. Alhamad, B. Z. Ergashevich, and N. J. Navimipour, 'Blockchain systems in embedded Internet of Things: Systematic literature review, challenges analysis, and future direction suggestions', Electronics, vol. 11, 2022.doi.org/10.3390/electronics11234020

[7] J. Pan, J. Wang, A. Hester, I. Alqerm, Y. Liu, and Y. Zhao, 'EdgeChain: An edge-IoT framework and prototype based on blockchain and smart contracts', IEEE Internet Things J, vol. 6, no. 3, pp. 4719-4732, June 2019.doi.org/10.1109/JIOT.2018.2878154

[8] M. Moudoud, S. Cherkaoui, and L. Khoukhi, "Towards a scalable and trustworthy blockchain: IoT use case," in Proc. IEEE Int. Conf. Commun. (ICC), Montreal, QC, Canada, Jun. 2021, pp. 1-6,doi.org/10.1109/ICC42927.2021.9500535

[9] Z. Wang, X. Liu, X. Shao, A. Alghamdi, M. Alrizq, M. S. Munir, and S. Biswas, "An optimized and scalable blockchain-based distributed learning platform for consumer IoT," Mathematics, vol. 11, no. 23, art. 4844, Dec. 2023,doi.org/10.3390/math11234844

[10] I. S. Ochôa et al., "Performance and security evaluation on a blockchain architecture for license plate recognition systems," Appl. Sci., vol. 11, no. 3, pp. 1255-1267, 2021.doi.org/10.3390/app11031255

[11] K. Godewatte Arachchige, P. Branch, and J. But, 'Evaluation of blockchain networks' scalability limitations in low-powered Internet of Things (IoT) sensor networks', Future Internet, vol. 15, no. 9, Sept. 2023.doi.org/10.3390/fi15090317

[12] E. U. Haque, A. Shah, J. Iqbal, S. S. Ullah, R. Alroobaea, and S. Hussain, "A scalable blockchain based framework for efficient IoT data management using lightweight consensus," Scientific Reports, vol. 14, no. 1, p. 7841, 2024, doi.org/10.1038/s41598-024-58578-7

[13] S. Bojjagani, B. R. Reddy, and B. S. Reddy, "IoT-based payment system using wearable devices," Int. J. Eng. Adv. Technol., vol. 11, no. 3, pp. 45-50, 2022.

[14] X. Xu, Z. Zeng, S. Yang, and H. Shao, "A novel blockchain framework for industrial IoT edge computing," Sensors, vol. 20, no. 7, p. 2061, 2020, doi.org/10.3390/s20072061

[15] R. Ch, I. Batra, and A. Malik, 'Block Chain based secure with improvised Bloom', Journal of Engineering Science & Technology Review, vol. 16, no. 2, pp. 123-130, 2023.doi.org/10.25103/jestr.162.16

[16] X. Lin, X. Shen, and J. Zhang, "A blockchain-based anonymous payment system with conditional anonymity," IEEE Trans. Inf. Forensics Secur., vol. 15, pp. 1-12, 2020. doi.org/10.1109/TIFS.2020.2969565

[17] S. Yoo, 'Blockchain based financial case analysis and its implications', Asia Pacific Journal of Innovation and Entrepreneurship, vol. 11, no. 3, pp. 312-321, 2017.doi.org/10.1108/APJIE-12-2017-036

[18] U. B. Chaudhry and A. K. Hydros, “Zero-trust-based security model against data breaches in the banking sector: A blockchain consensus algorithm,” *IET Blockchain*, vol. 3, no. 2, pp. 98–115, 2023, https://doi.org/10.1049/blc2.12028

[19] S. J. Rajawat, M. Kaushik, and S. K. Yadav, "Cloud enabled e-banking payment security implementation using blockchain technology," J. Electr. Syst., vol. 20, no. 7s, 2024.doi.org/10.52783/jes.3715

[20] J. Lin, M. Liu, S. Li, and X. Wang, SecurePay: Enabling secure and fast payment processing for platform economy. 2025.doi.org/10.1109/IWQoS65803.2025.11143297

[21] B. S. Rawal, G. Manogaran, and M. Hamdi, 'Multi tier stack of block chain with proxy re encryption method scheme on the Internet of Things platform', ACM Transactions on Internet Technology, vol. 22, no. 2, pp. 1-20, 2021.doi.org/10.1145/3421508

[22] S. Pandey, 'The influence of medical course experience on satisfaction, loyalty, and word-of-mouth in Indian medical colleges', Procedia Comput. Sci, vol. 132, pp. 84-91, 2018.doi.org/10.1016/j.procs.2018.05.165

[23] T. O. Sanyaolu, A. G. Adeleke, C. F. Azubuko, and O. S. Osundare, 'Harnessing blockchain technology in banking to enhance financial inclusion, security, and transaction efficiency', International Journal of Scholarly Research in Science and Technology, vol. 5, no. 1, pp. 35-053, 2024.doi.org/10.56781/ijsrst.2024.5.1.0032

[24] I. A. Hashimzai and M. Z. Ahmadzai, 'Navigating the integration of blockchain technology in banking: Opportunities and challenges', International Journal Software Engineering and Computer Science (IJSECS), vol. 4, no. 2, pp. 665-679, 2024. doi.org/10.35870/ijsecs.v4i2.2656

[25] T. O. Sanyaolu, A. G. Adeleke, C. F. Azubuko, and O. S. Osundare, 'Harnessing blockchain technology in banking to enhance financial inclusion, security, and transaction efficiency', Int. J. Scholarly Res. Sci. Technol, vol. 5, no. 1, pp. 35-53, 2024.doi.org/10.56781/ijsrst.2024.5.1.0032

How to Cite: Maimunatu Ya’u Ibrahim, Kabiru Ibrahim Musa, Aminu Ahmad. (2026). Security capabilities of blockchain technology on iot-based payment system. International Journal of Information Technology and Computer Engineering (IJITC), 6(1), 20-32. https://doi.org/10.55529/ijitc.61.20.32

BIOGRAPHIES OF AUTHORS

	Maimunatu Ya'u Ibrahim, is a final-year PhD student (awaiting Viva) in Management Information Technology at Abubakar Tafawa Balewa University (ATBU), Bauchi, where she also earned her B.Tech and M.Sc degrees in management information technology. Her research focuses on blockchain, IoT, and digital banking. She is currently employed with Gwani Software as the Head of the Project Management Unit. She has participated in numerous national and international conferences and written and co-authored twelve academic articles. A dedicated mentor in research writing and methodology, she supports student development in academia. She is a member of the Nigerian Computer Society and the Nigerian Institute of Management, contributing actively to both fields. She can be contacted at Email: yimaimunatu.pg@atbu.edu.ng
	Kabiru Ibrahim Musa, is an academic and IT professional with a PhD and MPhil from Essex, UK, and a Computer Science B.Sc. from ATBU. He is certified in Cisco Wireless, AWS, MCP, Huawei HCIE, and CCNA. Competent in MS SQL, MySQL, Postgres, and MongoDB, and skilled in Java, PHP, Python, JavaScript, DART, Flutter, AngularJS, and C#. He is a Senior Programmer at EasyICT Grid and an Associate Professor at ATBU. He has produced more than 48 publications and supervised more than 40 postgraduate students. His areas of expertise include web development, robotics, cloud computing, AI, network management, and cybersecurity. Additionally, he holds a certification as a Huawei Academic Instructor. He can be contacted at Email: imkabir@atbu.edu.ng
	Aminu Ahmad, is a Professor of Business Technology Management at ATBU Bauchi, holds a PhD in Technology Management, an MBA in Finance, and a B.Sc. in Business Administration. With over 27 years of experience, he has served as Dean, Head of Department, Special Adviser to the Minister of Communications, and Director at the NCC. He contributed to national digital policy through the National Broadband Implementation Steering Committee. A prolific researcher in technology management, innovation, and ICT adoption, he is a Fellow of the Academy of Management and a Certified Member of the International Strategic Management Institute, earning numerous awards for excellence. He can be contacted at Email: aminuahmad@atbu.edu.ng