Open Access Research Journal of
Engineering and Technology
Journals home page: https://oarjpublication/journals/oarjet/
ISSN: 2783-0128 (Online)

(REVIEW ARTICLE)

Blockchain technology as a paradigm shift in banking security: Theoretical and practical insights

Opeyemi Abayomi Odejide *

Independent Researcher, Hamilton, Ontario, Canada.

Open Access Research Journal of Engineering and Technology, 2024, 06(01), 052–062

Publication history: Received on 31 January 2024; revised on 18 March 2024; accepted on 20 March 2024

Article DOI: https://doi.org/10.53022/oarjet.2024.6.1.0013

Abstract

This paper explores the theoretical underpinnings of blockchain technology and its practical applications in enhancing banking security. The financial landscape is experiencing a seismic shift as disruptive technologies like blockchain emerge. Blockchain, with its core tenets of decentralization, immutability, and transparency, offers a transformative approach to banking security. This paper delves into the theoretical foundations of blockchain and explores its practical applications in bolstering bank security. Theoretical Underpinnings at its core, blockchain is a Distributed Ledger Technology (DLT). Imagine a digital record of transactions, not held by a single entity, but replicated and synchronized across a vast network of computers. This distributed nature eliminates the need for a central authority, fostering trust and transparency within the system. Cryptographic hashing adds another layer of security. Each transaction on the blockchain is cryptographically hashed, generating a unique fingerprint. This fingerprint is linked to the previous transaction's hash, creating an immutable chain of blocks. Any attempt to tamper with data would invalidate the entire chain, ensuring the integrity of every transaction. Consensus mechanisms play a vital role in ensuring network agreement. These mechanisms, like Proof of Work or Proof of Stake ensure all participants on the network agree on the validity of transactions and the current state of the ledger. Practical Applications in Banking Security**,** Traditional banking systems rely on centralized ledgers, susceptible to fraud and manipulation. Blockchain disrupts this paradigm by offering, Enhanced Transaction Security, by eliminating intermediaries and using cryptography, blockchain significantly reduces the risk of fraud and errors in financial transactions. The immutable nature of the ledger ensures transactions cannot be reversed or altered once recorded. Streamlined Regulatory Compliance**,** regulatory compliance is a constant challenge for banks. Blockchain simplifies the process by providing an auditable and transparent record of all transactions

Keywords: Decentralization; Immutability; Transparency; Cryptographic; Security Regulatory Compliance Cross-Border Payments

1. Introduction

The emergence of blockchain technology offers a transformative solution by creating a distributed ledger system that is secure, transparent, and tamper-proof. The Inevitable evolution, blockchain and the security of financial transactions, the financial sector, the lifeblood of global commerce, has long grappled with the critical issue of transaction security. For both banks and their customers, ensuring the safe and accurate movement of funds remains a paramount concern. Traditional banking systems, built upon centralized ledgers maintained by individual institutions, have inherent vulnerabilities (Oriekhoe et al., 2024).

These centralized systems are susceptible to fraud, errors, and manipulation. A single point of failure, whether a security breach or human error, can have devastating consequences. However, a transformative solution has emerged on the horizon blockchain technology. This revolutionary innovation promises to fundamentally reshape the landscape of financial security. At its core, blockchain operates on a distributed ledger system. Imagine a digital record of every

* Corresponding author: Opeyemi Abayomi Odejide

transaction, not locked away in a single vault, but replicated and synchronized across a vast network of computers (Egieya et al., 2023).

This decentralization eliminates the need for a central authority, a single point of vulnerability. Instead, trust and transparency are fostered within the system itself. The security of blockchain goes beyond its distributed nature. Every transaction on this digital ledger is cryptographically hashed, creating a unique fingerprint (Okorie et al., 2024). This fingerprint is then linked to the previous transaction's hash, forming an immutable chain of blocks. Tampering with any data within a block would be akin to trying to rewrite history, the entire chain would become invalid (Orieno et al., 2024).

This cryptographic security ensures the integrity of every transaction, forever etched in the digital ledger. The implications of blockchain technology for banking security are profound. Imagine a world where financial transactions are conducted with unparalleled security, eliminating the fear of fraud or errors. This is the future that blockchain promises, a future where trust is built into the very fabric of the financial system (Udeh et al., 2024).

1.1. Theoretical Foundations of Blockchain Technology

This distributed nature eliminates the need for a central authority to control the ledger, fostering trust and transparency Cryptographic Hashing, Each transaction on a blockchain is cryptographically hashed, generating a unique identifier. This hash is linked to the previous transaction's hash, creating an immutable chain of blocks. Tampering with any data within a block would invalidate the entire chain, ensuring data integrity (Okorie et al., 2024).

Consensus Mechanisms, Blockchain rely on consensus mechanisms to ensure agreement among network participants on the validity of transactions and the current state of the ledger. Popular consensus mechanisms include Proof of Work, Proof of Stake and Byzantine Fault Tolerance (BFT). The transformative potential of blockchain technology in banking security hinges on its core theoretical principles. This section delves into three fundamental concepts that underpin the secure and transparent nature of blockchain, Distributed Ledger Technology (DLT), Cryptographic Hashing, and Consensus Mechanisms (Oriekhoe et al., 2024).

Traditional banking systems rely on centralized ledgers. Each bank maintains its own record of transactions, creating a system prone to single points of failure and potential manipulation. DLT offers a revolutionary alternative. It refers to a digital database that is replicated and synchronized across a network of computers, geographically dispersed and independent of any central authority. This distributed architecture fosters several key benefits, Enhanced Trust and Transparency**,** With DLT, all participants in the network possess a copy of the ledger (Oriekhoe et al., 2024).

This fosters trust as there's no single entity controlling the data. Everyone can verify the validity of transactions, promoting transparency within the system. Reduced Risk of Fraud, Centralized ledgers create a vulnerability as a single point of entry for malicious actors. DLT mitigates this risk by distributing the ledger across a vast network. It becomes incredibly difficult to manipulate the data without detection by the entire network. Increased Resilience**,** Centralized systems are susceptible to outages or disruptions (Adaga et al., 2023).

DLT boasts enhanced resilience as the ledger remains accessible even if individual nodes within the network experience downtime. Transactions can still be processed and verified by the remaining active nodes. Improved Auditability, Every change made to the DLT is recorded and reflected in all copies of the ledger. This comprehensive audit trail facilitates easier identification and resolution of potential errors or discrepancies. DLT establishes a secure foundation for blockchain, but it requires a mechanism to ensure the immutability of data within each transaction (Nwokediegwu et al., 2024).

This is where cryptographic hashing comes into play. It is a cryptographic function that transforms any digital data into a unique and fixed-size string of characters, called a hash.

There are two crucial properties of cryptographic hashes that make them ideal for blockchain security, Uniqueness**,** Two different pieces of data will always produce distinct hashes.

Determinism**,** providing the same input data will always generate the same hash output. These properties are leveraged in a way that safeguards the integrity of each transaction on the blockchain. Imagine each transaction as a block (Daudu et al., 2024).

Each block contains data (e.g., transaction details), a timestamp, and a crucial element, the hash of the previous block. When a new transaction is added to the blockchain, a new block is created. This new block not only contains the current transaction data but also includes the hash of the previous block in the chain. Any attempt to tamper with data within a block would result in a change in its hash. However, this change would also invalidate the hash of the subsequent block, and so on, all the way back to the beginning of the chain (Ayorinde et al., 2024).

This chain of hashes creates an immutable record, making it nearly impossible to alter data on the blockchain without detection. While DLT and cryptographic hashing provide a robust foundation for data security, a critical question remains, how do participants in a decentralized network agree on the validity of transactions and the current state of the ledger? This is where consensus mechanisms come into play (Nwokediegwu et al., 2024). These mechanisms are a set of rules that govern how participants in the blockchain network reach agreement on the following, Transaction Validity, Consensus mechanisms ensure that only legitimate transactions are added to the blockchain.

They prevent double-spending or the inclusion of fraudulent transactions.

Current State of the Ledger**,** with multiple copies of the DLT distributed across the network, there's a need to ensure all copies are synchronized and reflect the same state of transactions. Popular consensus mechanisms include Proof of Work. This mechanism uses a computationally intensive process to validate transactions. Miners compete to solve complex mathematical puzzles, and the first miner to find a solution gets to add the next block to the chain (Usiagu et al., 2024)

This process secures the network as modifying the blockchain would require immense computational power, making it impractical for malicious actors. However, POW can be energy-intensive and slow for high-volume transactions. Proof of Stake. This mechanism selects validators based on their stake in the crypto currency associated with the blockchain. Validators are responsible for verifying transactions and adding new blocks Byzantine Fault Tolerance (BFT), this mechanism allows the network to reach consensus even in the presence of a limited number of faulty or malicious nodes (Daudu et al., 2024)

1.2. Practical Applications of Blockchain in Banking Security

Enhanced Transaction Security, Blockchain eliminates the need for intermediaries in financial transactions, reducing the risk of fraud and errors. The immutable nature of the blockchain ensures that transactions cannot be reversed or altered once recorded. Improved Regulatory Compliance, Regulatory compliance remains a significant challenge for banks. Blockchain can streamline compliance processes by providing a transparent and auditable record of all transactions (Ayorinde et al., 2024).

Regulatory authorities can access relevant data efficiently, reducing administrative burdens for banks. Strengthened Identity Management, Blockchain can be leveraged to create secure and tamper-proof digital identities. This can improve customer onboarding processes and reduce the risk of identity theft, a growing concern in the digital age (Adefemi et al., 2024). Cross-Border Payments, Traditional cross-border payments are often slow and expensive due to intermediary banks and complex regulations. Blockchain-based solutions can expedite cross-border transactions by eliminating intermediaries and streamlining the process (Usiagu et al., 2024).

The theoretical foundations of blockchain technology, as explored in the previous section, provide a powerful framework for enhancing security within the financial sector. This section delves into the practical applications of blockchain that are revolutionizing banking security across several key areas. Enhanced Transaction Security, Traditional banking systems rely on intermediaries like correspondent banks to facilitate financial transactions. This introduces vulnerabilities as each intermediary adds another layer of complexity and potential points of failure. Blockchain disrupts this model by enabling direct peer-to-peer (P2P) transactions between banks or even individual users (Okoli et al., 2024).

This eliminates the need for intermediaries, significantly reducing the risk of fraud**,** Reduced Fraudulent Activity, with intermediaries out of the picture, opportunities for fraudulent activities like transaction manipulation or unauthorized access are minimized. P2P transactions are directly recorded on the immutable blockchain, making them tamper-proof and readily verifiable by all participants. Elimination of Double Spending**,** Double spending, the fraudulent act of using the same digital asset twice, is a significant concern in traditional systems (Etukudoh et al., 2024).

Block chain's immutability ensures that every transaction is recorded only once and cannot be reversed or altered. This inherent property eliminates the possibility of double spending in the blockchain environment. Regulatory compliance

is a constant challenge for banks, requiring them to maintain a meticulous record of all transactions and adhere to stringent anti-money laundering (AML) and Know Your Customer (KYC) regulations. Blockchain offers a transformative solution by providing a secure and auditable record of all transactions, Streamlined Reporting, The immutable nature of the blockchain creates a readily accessible, chronological record of all transactions (Ochuba et al., 2024).

Regulatory authorities can efficiently access relevant data for audits and investigations, reducing the administrative burden on banks in generating compliant reports. Enhanced Transparency and Traceability**,** All transactions on the blockchain are transparent and traceable, providing regulators with a clear view of the flow of funds. This fosters greater transparency within the financial system and aids in combating illicit activities (Okafor et al., 2024). Automated Regulatory Checks, Smart contracts, self-executing contracts programmed on the blockchain, can be designed to automatically verify transactions against AML and KYC regulations.

This reduces the need for manual compliance checks and expedites the transaction process. Identity theft remains a significant threat in the digital age. Traditional methods of identity verification often rely on centralized databases that can be susceptible to breaches. Blockchain offers a secure and tamper-proof alternative for managing digital identities, Self-Sovereign Identity (SSI), Blockchain enables the creation of SSI, where users control their own digital identities. This eliminates the need to rely on centralized authorities and reduces the risk of identity theft (Amoo et al., 2024).

Verifiable Credentials**,** Individuals can store verifiable credentials, such as educational certificates or employment records, on the blockchain. These credentials can be easily shared and verified, streamlining processes and reducing reliance on paper documents**.** Enhanced Customer Onboarding, Blockchain-based identity verification can streamline customer onboarding processes for banks. Customers can securely share verified credentials, expediting account creation and mitigating risks associated with fraudulent identities (Ochuba et al., 2024).

Cross-border payments are often plagued by slow processing times and high fees due to multiple intermediaries, complex regulations, and currency conversions involved. Blockchain offers a solution for faster and more cost-effective international transactions, Reduced Intermediaries**,** Blockchain eliminates the need for intermediary banks, significantly reducing transaction processing times and associated costs. P2P transactions happen directly between parties, leading to faster settlements (Usman et al., 2024).

Streamlined Regulatory Processes, Smart contracts can be programmed to automatically trigger regulatory checks on cross-border transactions, eliminating delays associated with manual verifications. This facilitates faster compliance and expedites transaction settlements. Increased Transparency and Traceability**,** The transparency of blockchain allows for clear tracking of cross-border payments, reducing the risk of errors and fraud. Regulatory authorities can monitor transactions efficiently, enhancing financial stability and security (Akinrinola et al., 2024).

Beyond the aforementioned areas, blockchain technology has the potential to revolutionize other aspects of banking security, Trade Finance, Blockchain can streamline trade finance processes by providing a secure and transparent platform for managing trade documents and facilitating payments between exporters and importers. Securities Trading**,** Blockchain can enable faster and more efficient settlements in securities trading by eliminating reconciliation issues and streamlining ownership records. Supply Chain Management, Blockchain can be leveraged to track the movement of goods throughout a supply chain, enhancing transparency and security for all stakeholders involved (Adaga et al., 2024).

1.3. Challenges and Consideration

The regulatory landscape surrounding blockchain technology is still evolving. Banks need to navigate regulatory uncertainties while exploring the potential of blockchain for enhancing security. The lack of standardized protocols across different blockchain platforms can hinder interoperability between banks. Collaborative efforts are underway to establish industry-wide standards for blockchain adoption in banking embracing the Potential While Addressing the Hurdles (Abrahams et al., 2023)

While the transformative potential of blockchain technology in banking security is undeniable, significant challenges and considerations must be addressed before widespread adoption becomes a reality. This section delves into three critical areas that demand attention, scalability, regulation, and standardization. Existing blockchain platforms face a significant hurdle scalability. They were not initially designed to handle the high transaction volumes typical of large-scale banking operations (Hassan et al., 2024).

Traditional financial systems can process thousands of transactions per second, whereas many popular blockchain platforms struggle to handle a mere handful. This limitation poses a critical challenge for integrating blockchain into

core banking functionalities. Blockchain rely on a block-based structure. Each block can only hold a limited amount of data. This limitation restricts the number of transactions that can be processed per block. Consensus Mechanisms, Consensus mechanisms like Proof of Work require significant computational resources, leading to slow transaction processing times (Abrahams et al., 2024).

This is particularly problematic for high-volume banking applications. Addressing Scalability Challenges, Research efforts are actively underway to develop scalable blockchain solutions suitable for the banking industry. Some promising approaches include, Increased Block Size, while increasing block size can accommodate more transactions, it can also lead to centralization issues and longer block confirmation times. Finding an optimal balance is these solutions operate on top of existing blockchain, handling a large volume of transactions off-chain and periodically syncing with the main chain (Atadoga et al., 2024).

This reduces the burden on the main chain and improves scalability. Alternative Consensus Mechanisms**,** Consensus mechanisms like Proof of Stake require less computational power than, potentially leading to faster transaction processing times. Exploring and adapting alternative mechanisms suited for high-throughput environments is key. The regulatory landscape surrounding blockchain technology is still evolving. While regulators recognize the potential benefits of blockchain for the financial sector, there are uncertainties regarding how existing regulations will apply to this new paradigm (Osasona et al., 2024).

This creates a challenge for banks, who need to be compliant with regulatory requirements while exploring the potential of blockchain, Consumer Protection, Regulatory frameworks need to address potential consumer protection issues related to data privacy and security in the context of blockchain. Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT), Regulators need to develop strategies to identify and mitigate potential risks of money laundering and terrorist financing associated with anonymity features of some blockchain platforms (Reis et al., 2024)

Open communication and collaboration with regulatory bodies are crucial. Banks can share their insights and concerns about blockchain while seeking clarification on relevant regulations. Phased Implementation**,** A phased approach to blockchain adoption allows banks to test and refine their solutions in a controlled environment while ensuring compliance with existing regulations**.** Industry Standards, Participating in industry-wide efforts to develop standardized approaches to AML/KYC compliance and consumer protection on blockchain can facilitate regulatory clarity and expedite adoption (Anyanwu et al., 2024).

The lack of standardized protocols across different blockchain platforms poses yet another challenge. This creates a barrier to interoperability between banks, hindering the potential benefits of a truly interconnected financial ecosystem Interoperability Challenges, Banks using different blockchain platforms may struggle to communicate and transact with each other seamlessly. This can limit the potential network effects and broader adoption of blockchain technology within the banking sector (Abrahams et al., 2024).

Technical Complexity, Developing and maintaining interoperable blockchain platforms requires complex technical solutions and coordinated efforts across industry stakeholders. Forging a Path to Interoperability**,** Industry-wide collaboration and the development of open standards are key to over, Standardization Initiatives, Collaborative efforts like the Hyper ledger Project are spearheading the development of interoperable blockchain protocols, paving the way for seamless communication between different platforms (Adaga et al., 2024).

Interoperability Frameworks, Establishing technical frameworks that facilitate smooth data exchange between different blockchain platforms is critical for achieving interoperability. Consortia and Partnerships**,** Banks and technology companies can join forces in consortia and partnerships to develop and implement interoperable blockchain solutions. Scalability, regulation, and standardization are sinificant hurdles on the path towards widespread blockchain adoption in banking security. However, ongoing research and industry collaboration are fostering solutions to address these challenges (Abrahams et al., 2024)

1.4. Case Studies

Ripple Net is a blockchain-based platform designed for cross-border payments. It enables banks to settle transactions directly with each other in real-time, reducing costs and transaction times. JPMorgan Chase's Interbank Information Network (IIN), IIN is a consortium-based blockchain platform developed by JPMorgan Chase to improve information sharing and streamline processes between banks. The theoretical foundations and practical applications of blockchain technology within banking security paint a compelling picture of a transformative future (Amoo et al., 2024).

However, to truly understand the impact of blockchain, it's crucial to examine real-world examples. This section delves into two prominent case studies showcasing how blockchain is already revolutionizing security in the banking sector, Ripple Net, Transforming Cross-Border Payment Traditional cross-border payments are notorious for being slow, expensive, and opaque. Intermediary banks, complex regulations, and lengthy currency conversion processes often lead to delays and high fees (Okoli et al., 2024).

Ripple Net, a blockchain-based platform developed by Ripple, is tackling these challenges head-on, improving cross-border payment security and efficiency. Ripple Net leverages the power of blockchain technology to create a secure and transparent network for banks to settle transactions directly with each other. Here's how it streamlines cross-border payments**,** Faster Settlements, Ripple Net utilizes the XRP crypto currency as a settlement mechanism. Transactions are settled on the blockchain in seconds, significantly faster than traditional methods that can take days (McLaughlin, 2024).

Reduced Costs**,** Eliminating intermediary banks removes associated fees, leading to cost savings for both banks and their customers. All participants in the network can track the progress of a transaction in real-time, fostering transparency and reducing the risk of errors or delays. Proved Security, The immutable nature of the blockchain ensures the security of transactions (McGurk and Reichenbach, 2024).

Impact on Banking Security, Ripple Net directly addresses a significant vulnerability in traditional banking the slow and insecure nature of cross-border transactions. By facilitating faster settlements, reducing costs, and enhancing transparency, Ripple Net offers a secure and efficient alternative. This fosters trust within the financial ecosystem and mitigates security risks associated with delays and potential fraud in traditional cross-border transactions (Surve and Nguyen, 2024).

JPMorgan Chase, a leading global financial institution, has recognized the potential of blockchain technology to improve internal processes and information sharing within the banking sector. The Interbank Information Network (IIN) is a consortium-based blockchain platform developed by JPMorgan Chase to address these challenges. IN is a permissioned blockchain network specifically designed for information sharing between banks. Banks can securely share data on known-your-customer (KYC) information, trade finance documents, and other critical data points within the network (Alirezaie et al., 2024).

Here's how IIN improves information exchange, Enhanced Security**,** Data on the IIN platform is encrypted and immutable, ensuring the security and integrity of shared information. Streamlined Processes, The secure and efficient sharing of data facilitates faster completion of KYC checks and trade finance transactions, improving operational efficiency. Reduced Costs, Streamlining information sharing and automating processes minimizes manual efforts and associated operational costs for banks (Abildtrup, 2024).

Impact on Banking Security**,** The IIN platform addresses another critical aspect of banking security, the secure and efficient exchange of information between banks. Traditional methods of information sharing are often cumbersome and susceptible to errors. IIN enhances security by using block chain’s immutability to protect sensitive data. Streamlined processes and improved data quality contribute to a more secure banking environment by reducing vulnerabilities associated with information discrepancies and fraud.

1.5. Future Outlook, Embracing a More Secure Future

The theoretical foundations, practical applications, and real-world case studies paint a clear picture, blockchain technology has the potential to revolutionize the future of banking security (Aripin, 2024). While challenges regarding scalability, regulation, and standardization remain, ongoing research and collaboration are paving the way for widespread adoption. Scalability Enhancements, Ongoing research and development are focusing on advancements in consensus mechanisms and layer-2 solutions to increase transaction processing capabilities of blockchain platforms (Yusoff and Abd Ali, 2024).

Regulatory bodies are actively engaging with blockchain industry stakeholders to develop a clear framework for governing the technology within the financial Collaborative efforts aiming to establish interoperable protocols and standardized approaches to compliance will facilitate seamless integration of blockchain across the banking ecosystem Benefits of Widespread Adoption, Enhanced Security**,** The immutable and tamper-proof nature of blockchain transactions will lead to a more secure financial system, reducing fraud and errors Increased Efficiency, Streamlined transaction processing, faster cross-border payments, and automated compliance checks will lead to significant efficiency gains for banks (Addula et al., 2023).

Transformative Power, Standardization**,** and The lack of standardized protocols across different blockchain platforms hinders interoperability between banks (Alamsya and Syahrir, 2024). Industry-wide efforts to develop interoperable platforms and standardized approaches to security and compliance are essential for widespread adoption. The future of banking security holds immense promise with the integration of blockchain technology. As research progresses, scalability limitations are addressed, and regulatory frameworks evolve, widespread adoption becomes a realistic possibility (Morris and Brubaker, 2024).

Advancements in Scalability, Ongoing research on consensus mechanisms and layer-2 solutions aims to increase transaction processing capabilities of blockchain platforms, making them suitable for high-volume banking application Evolving Regulatory Landscape**,** Regulatory bodies are actively engaging with the blockchain industry to develop clear frameworks for governing the technology within the financial sector. This fosters trust and facilitates the responsible integration of blockchain into banking operations. Standardization Efforts, Collaboration across industry stakeholders is crucial for establishing interoperable protocols and standardized approaches to security and compliance (Asaju, 2024).

This enables seamless integration of blockchain technology across the banking ecosystem. Benefits of Widespread Adoption for Banks, Enhanced Security**,** by leveraging the immutability of blockchain, banks can create a more secure financial environment, mitigating fraud and errors associated with traditional systems (Labu and Ahammed, 2024). Increased Efficiency**,** Streamlined transaction processing, faster cross-border payments, and automated compliance checks will lead to significant efficiency gains for banks, reducing operational costs and improving service delivery (Craig et al., 2024).

2. Conclusion

The financial sector stands at the precipice of a transformative era. Blockchain technology, with its core principles of decentralization, immutability, and transparency, offers a paradigm shift in banking security. This paper has delved into the theoretical foundations and practical applications of blockchain, exploring how it can revolutionize the way financial transactions are conducted and secured. Enhanced Security, Traditional banking systems are vulnerable to fraud, errors, and manipulation. Blockchain eliminates intermediaries, reducing opportunities for malicious activities. The immutable nature of the ledger ensures data integrity and prevents unauthorized modifications**.** Improved Regulatory Compliance**,** Regulatory compliance remains a constant burden for banks. Blockchain provides a secure and auditable record of all transactions, simplifying compliance processes and reducing administrative costs. Strengthened Identity Management, Blockchain empowers individuals to control their own digital identities, mitigating risks associated with identity theft. Verifiable credentials stored on the blockchain streamline customer onboarding and enhance trust within the system Faster and More Efficient Cross-Border Payments, Traditional cross-border payments are slow and expensive due to intermediaries and complex regulations. Blockchain facilitates direct peer-to-peer transactions, eliminating intermediaries and streamlining the process. Blockchain technology represents a paradigm shift in banking security. While challenges remain, the potential benefits are undeniable. By embracing this transformative technology, banks can create a more secure, transparent, and efficient financial ecosystem, paving the way for a future where financial transactions are conducted with greater trust and security.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

Reference

[1] Abildtrup, A., 2024. The Rise of Robotic Process Automation in the Banking Sector: Streamlining Operations and Improving Efficiency.

[2] Abrahams, T.O., Ewuga, S.K., Kaggwa, S., Uwaoma, P.U., Hassan, A.O. and Dawodu, S.O., 2023. Review of strategic alignment: Accounting and cybersecurity for data confidentiality and financial security.

[3] Abrahams, T.O., Ewuga, S.K., Kaggwa, S., Uwaoma, P.U., Hassan, A.O. and Dawodu, S.O., 2024. Mastering compliance: a comprehensive review of regulatory frameworks in accounting and cybersecurity. *Computer Science & IT Research Journal*, *5*(1), pp.120-140.

[4] Abrahams, T.O., Farayola, O.A., Amoo, O.O., Ayinla, B.S., Osasona, F. and Atadoga, A., 2024. Continuous improvement in information security: A review of lessons from superannuation cybersecurity uplift programs. *International Journal of Science and Research Archive*, *11*(1), pp.1327-1337.

[5] Abrahams, T.O., Farayola, O.A., Kaggwa, S., Uwaoma, P.U., Hassan, A.O. and Dawodu, S.O., 2024. CYBERSECURITY AWARENESS AND EDUCATION PROGRAMS: A REVIEW OF EMPLOYEE ENGAGEMENT AND ACCOUNTABILITY. *Computer Science & IT Research Journal*, *5*(1), pp.100-119.

[6] Abrahams, T.O., Farayola, O.A., Kaggwa, S., Uwaoma, P.U., Hassan, A.O. and Dawodu, S.O., 2024. REVIEWING THIRD-PARTY RISK MANAGEMENT: BEST PRACTICES IN ACCOUNTING AND CYBERSECURITY FOR SUPERANNUATION ORGANIZATIONS. *Finance & Accounting Research Journal*, *6*(1), pp.21-39.

[7] Adaga, E.M., Egieya, Z.E., Ewuga, S.K., Abdul, A.A. and Abrahams, T.O., 2024. Philosophy in business analytics: a review of sustainable and ethical approaches. *International Journal of Management & Entrepreneurship Research*, *6*(1), pp.69-86.

[8] Adaga, E.M., Egieya, Z.E., Ewuga, S.K., Abdul, A.A. and Abrahams, T.O., 2024. A COMPREHENSIVE REVIEW OF ETHICAL PRACTICES IN BANKING AND FINANCE. *Finance & Accounting Research Journal*, *6*(1), pp.1-20.

[9] Adaga, E.M., Egieya, Z.E., Ewuga, S.K., Abdul, A.A. and Abrahams, T.O., 2024. TACKLING ECONOMIC INEQUALITIES THROUGH BUSINESS ANALYTICS: A LITERATURE REVIEW. *Computer Science & IT Research Journal*, *5*(1), pp.60-80.

[10] Adaga, E.M., Okorie, G.N., Egieya, Z.E., Ikwue, U., Udeh, C.A., DaraOjimba, D.O. and Oriekhoe, O.I., 2023. THE ROLE OF BIG DATA IN BUSINESS STRATEGY: A CRITICAL REVIEW. *Computer Science & IT Research Journal*, *4*(3), pp.327-350.

[11] Addula, S.R., Meduri, K., Nadella, G.S. and Gonaygunta, H., AI and Blockchain in Finance: Opportunities and Challenges for the Banking Sector.

[12] Adefemi, A., Daudu, C.D., Okoli, C.E., Ayorinde, O.B., Adekoya, O.O. and Ibeh, C.V., 2024. Reviewing the development of floating LNG facilities and their global impact.

[13] Alamsyah, A. and Syahrir, S., 2024. A Taxonomy on Blockchain-Based Technology in the Financial Industry: Drivers, Applications, Benefits, and Threats. In *Blockchain and Smart-Contract Technologies for Innovative Applications* (pp. 91-129). Springer, Cham.

[14] Alirezaie, M., Hoffman, W., Zabihi, P., Rahnama, H. and Pentland, A., 2024. Decentralized Data and Artificial Intelligence Orchestration for Transparent and Efficient Small and Medium-Sized Enterprises Trade Financing. *Journal of Risk and Financial Management*, *17*(1), p.38.

[15] Amoo, O.O., Atadoga, A., Osasona, F., Abrahams, T.O., Ayinla, B.S. and Farayola, O.A., 2024. GDPR's impact on cybersecurity: A review focusing on USA and European practices. *International Journal of Science and Research Archive*, *11*(1), pp.1338-1347.

[16] Amoo, O.O., Osasona, F., Atadoga, A., Ayinla, B.S., Farayola, O.A. and Abrahams, T.O., 2024. Cybersecurity threats in the age of IoT: A review of protective measures. *International Journal of Science and Research Archive*, *11*(1), pp.1304-1310.

[17] Anyanwu, A., Olorunsogo, T., Abrahams, T.O., Akindote, O.J. and Reis, O., 2024. DATA CONFIDENTIALITY AND INTEGRITY: A REVIEW OF ACCOUNTING AND CYBERSECURITY CONTROLS IN SUPERANNUATION ORGANIZATIONS. *Computer Science & IT Research Journal*, *5*(1), pp.237-253.

[18] Aripin, Z., Saepudin, D. and Yulianty, F., 2024, February. TRANSFORMATION IN THE INTERNET OF THINGS (IOT) MARKET IN THE BANKING SECTOR: A CASE STUDY OF TECHNOLOGY IMPLEMENTATION FOR SERVICE IMPROVEMENT AND TRANSACTION SECURITY. In *Journal of Jabar Economic Society Networking Forum* (Vol. 1, No. 3, pp. 17-32).

[19] Asaju, B.J., 2024. Standardization and Regulation of V2X Cybersecurity: Analyzing the Current Landscape, Identifying Gaps, and Proposing Frameworks for Harmonization. *Advances in Deep Learning Techniques*, *4*(1), pp.33-52.

[20] Atadoga, A., Farayola, O.A., Ayinla, B.S., Amoo, O.O., Abrahams, T.O. and Osasona, F., 2024. A COMPARATIVE REVIEW OF DATA ENCRYPTION METHODS IN THE USA AND EUROPE. *Computer Science & IT Research Journal*, *5*(2), pp.447-460.

[21] Ayinla, B.S., Amoo, O.O., Atadoga, A., Abrahams, T.O., Osasona, F. and Farayola, O.A., 2024. Ethical AI in practice: Balancing technological advancements with human values. *International Journal of Science and Research Archive*, *11*(1), pp.1311-1326.

[22] Ayorinde, O.B., Daudu, C.D., Etukudoh, E.A., Adefemi, A., Adekoya, O.O. and Okoli, C.E., 2024. CLIMATE RISK ASSESSMENT IN PETROLEUM OPERATIONS: A REVIEW OF CSR PRACTICES FOR SUSTAINABLE RESILIENCE IN THE UNITED STATES AND AFRICA. *Engineering Science & Technology Journal*, *5*(2), pp.385-401.

[23] Ayorinde, O.B., Daudu, C.D., Okoli, C.E., Adefemi, A., Adekoya, O.O. and Ibeh, C.V., 2024. Reviewing the impact of LNG technology advancements on global energy markets.

[24] Ayorinde, O.B., Etukudoh, E.A., Nwokediegwu, Z.Q.S., Ibekwe, K.I., Umoh, A.A. and Hamdan, A., 2024. Renewable energy projects in Africa: A review of climate finance strategies. *International Journal of Science and Research Archive*, *11*(1), pp.923-932.

[25] Craig, S., Pinero, L., Terry, A. and Lindsey, B., 2024, March. Automation–Continuing to Improve Service Delivery of Coiled Tubing Operations. In *SPE/ICoTA Well Intervention Conference and Exhibition* (p. D011S002R001). SPE.

[26] Daudu, C.D., Adefemi, A., Adekoya, O.O., Okoli, C.E., Ayorinde, O.B. and Daraojimba, A.I., 2024. LNG AND CLIMATE CHANGE: EVALUATING ITS CARBON FOOTPRINT IN COMPARISON TO OTHER FOSSIL FUELS. *Engineering Science & Technology Journal*, *5*(2), pp.412-426.

[27] Daudu, C.D., Okoli, C.E., Adefemi, A., Ayorinde, O.B., Adekoya, O.O. and Daraojimba, A.I., 2024. Reviewing the economic viability of LNG projects in African Nations.

[28] Egieya, Z.E., Ewuga, S.K., Omotosho, A., Adegbite, A.O. and Oriekhoe, O.I., 2023. A review of sustainable entrepreneurship practices and their impact on long-term business viability. *World Journal of Advanced Research and Reviews*, *20*(3), pp.1283-1292.

[29] Etukudoh, E.A., Ilojianya, V.I., Ayorinde, O.B., Daudu, C.D., Adefemi, A. and Hamdan, A., 2024. Review of climate change impact on water availability in the USA and Africa. *International Journal of Science and Research Archive*, *11*(1), pp.942-951.

[30] Hassan, A.O., Ewuga, S.K., Abdul, A.A., Abrahams, T.O., Oladeinde, M. and Dawodu, S.O., 2024. Cybersecurity in banking: a global perspective with a focus on Nigerian practices. *Computer Science & IT Research Journal*, *5*(1), pp.41-59.

[31] Labu, M.R. and Ahammed, M.F., 2024. Next-Generation Cyber Threat Detection and Mitigation Strategies: A Focus on Artificial Intelligence and Machine Learning. *Journal of Computer Science and Technology Studies*, *6*(1), pp.179-188.

[32] McGurk, B. and Reichenbach, S., 2024. The application of DLT in financial services: Benefits and use cases. In *Financial Services Law and Distributed Ledger Technology* (pp. 64-90). Edward Elgar Publishing.

[33] McLaughlin, D., 2024. Remarks on Blockchain and Distributed Ledger Technology in Financial Market Infrastructures. *Available at SSRN 4745315*.

[34] Morris, M.R. and Brubaker, J.R., 2024. Generative ghosts: Anticipating benefits and risks of AI afterlives. *arXiv preprint arXiv:2402.01662*.

[35] Nwokediegwu, Z.Q.S., Adefemi, A., Ayorinde, O.B., Ilojianya, V.I. and Etukudoh, E.A., 2024. REVIEW OF WATER POLICY AND MANAGEMENT: COMPARING THE USA AND AFRICA. *Engineering Science & Technology Journal*, *5*(2), pp.402-411.

[36] Nwokediegwu, Z.Q.S., Ibekwe, K.I., Ilojianya, V.I., Etukudoh, E.A. and Ayorinde, O.B., 2024. RENEWABLE ENERGY TECHNOLOGIES IN ENGINEERING: A REVIEW OF CURRENT DEVELOPMENTS AND FUTURE PROSPECTS. *Engineering Science & Technology Journal*, *5*(2), pp.367-384.

[37] Ochuba, N.A., Amoo, O.O., Akinrinola, O., Usman, F.O. and Okafor, E.S., 2024. MARKET EXPANSION AND COMPETITIVE POSITIONING IN SATELLITE TELECOMMUNICATIONS: A REVIEW OF ANALYTICS-DRIVEN STRATEGIES WITHIN THE GLOBAL LANDSCAPE. *International Journal of Management & Entrepreneurship Research*, *6*(3), pp.567-58.

[38] Ochuba, N.A., Amoo, O.O., Okafor, E.S., Usman, F.O. and Akinrinola, O., 2024. CONCEPTUAL DEVELOPMENT AND FINANCIAL ANALYTICS FOR STRATEGIC DECISION-MAKING IN TELECOMMUNICATIONS, FOCUSING ON ASSESSING INVESTMENT OPPORTUNITIES AND MANAGING RISKS IN SATELLITE PROJECTS. *International Journal of Management & Entrepreneurship Research*, *6*(3), pp.594-607.

[39] Ochuba, N.A., Okafor, E.S., Akinrinola, O., Amoo, O.O. and Usman, F.O., 2024. ENHANCING CUSTOMER SERVICE IN SATELLITE TELECOMMUNICATIONS: A REVIEW OF DATA-DRIVEN INSIGHTS AND METHODOLOGIES FOR PERSONALIZED SERVICE OFFERINGS. *International Journal of Management & Entrepreneurship Research*, *6*(3), pp.582-593.

[40] Ochuba, N.A., Okafor, E.S., Akinrinola, O., Usman, F.O. and Amoo, O.O., 2024. STRATEGIC PARTNERSHIPS IN THE SATELLITE AND TELECOMMUNICATIONS SECTORS: A CONCEPTUAL REVIEW OF DATA ANALYTICS-ENABLED IDENTIFICATION AND CAPITALIZATION OF SYNERGIES. *Engineering Science & Technology Journal*, *5*(3), pp.716-727.

[41] Ochuba, N.A., Usman, F.O., Amoo, O.O., Okafor, E.S. and Akinrinola, O., 2024. INNOVATIONS IN BUSINESS MODELS THROUGH STRATEGIC ANALYTICS AND MANAGEMENT: CONCEPTUAL EXPLORATION FOR SUSTAINABLE GROWTH. *International Journal of Management & Entrepreneurship Research*, *6*(3), pp.554-566.

[42] Ochuba, N.A., Usman, F.O., Okafor, E.S., Akinrinola, O. and Amoo, O.O., 2024. PREDICTIVE ANALYTICS IN THE MAINTENANCE AND RELIABILITY OF SATELLITE TELECOMMUNICATIONS INFRASTRUCTURE: A CONCEPTUAL REVIEW OF STRATEGIES AND TECHNOLOGICAL ADVANCEMENTS. *Engineering Science & Technology Journal*, *5*(3), pp.704-715.

[43] Okafor, E.S., Akinrinola, O., Usman, F.O., Amoo, O.O. and Ochuba, N.A., 2024. CYBERSECURITY ANALYTICS IN PROTECTING SATELLITE TELECOMMUNICATIONS NETWORKS: A CONCEPTUAL DEVELOPMENT OF CURRENT TRENDS, CHALLENGES, AND STRATEGIC RESPONSES. *International Journal of Applied Research in Social Sciences*, *6*(3), pp.254-266.

[44] Okoli, C.E., Adekoya, O.O., Ilojianya, V.I., Ayorinde, O.B., Etukudoh, E.A. and Hamdan, A., 2024. Sustainable energy transition strategies: A comparative review of CSR and corporate advising in the petroleum industry in the United States and Africa. *International Journal of Science and Research Archive*, *11*(1), pp.933-941.

[45] Okoli, U.I., Obi, O.C., Adewusi, A.O. and Abrahams, T.O., 2024. Machine learning in cybersecurity: A review of threat detection and defense mechanisms.

[46] Okorie, G.N., Egieya, Z.E., Ikwue, U., Udeh, C.A., Adaga, E.M., DaraOjimba, O.D. and Oriekhoe, O.I., 2024. LEVERAGING BIG DATA FOR PERSONALIZED MARKETING CAMPAIGNS: A REVIEW. *International Journal of Management & Entrepreneurship Research*, *6*(1), pp.216-242.

[47] Okorie, G.N., Udeh, C.A., Adaga, E.M., DaraOjimba, O.D. and Oriekhoe, O.I., 2024. DIGITAL MARKETING IN THE AGE OF IOT: A REVIEW OF TRENDS AND IMPACTS. *International Journal of Management & Entrepreneurship Research*, *6*(1), pp.104-131.

[48] Oriekhoe, O.I., Addy, W.A., Okoye, C.C., Oyewole, A.T., Ofodile, O.C. and Ugochukwu, C.E., 2024. The role of accounting in mitigating food supply chain risks and food price volatility. *International Journal of Science and Research Archive*, *11*(1), pp.2557-2565.

[49] Oriekhoe, O.I., Ashiwaju, B.I., Ihemereze, K.C., Ikwue, U. and Udeh, C.A., 2024. Review Of Technological Advancements In Food Supply Chain Management: A Comparative Study Between The Us And Africa. *International Journal of Management & Entrepreneurship Research*, *6*(1), pp.132-149.

[50] Oriekhoe, O.I., Ashiwaju, B.I., Ihemereze, K.C., Ikwue, U. and Udeh, C.A., 2023. Review of technological advancement in food supply chain management: comparison between USA and Africa. *World Journal of Advanced Research and Reviews*, *20*(3), pp.1681-1693.

[51] Oriekhoe, O.I., Ashiwaju, B.I., Ihemereze, K.C., Ikwue, U. and Udeh, C.A., 2024. REVIEW OF INNOVATIVE SUPPLY CHAIN MODELS IN THE US PHARMACEUTICAL INDUSTRY: IMPLICATIONS AND ADAPTABILITY FOR AFRICAN HEALTHCARE SYSTEMS. *International Medical Science Research Journal*, *4*(1), pp.1-18.

[52] Oriekhoe, O.I., Oyeyemi, O.P., Bello, B.G., Omotoye, G.B., Daraojimba, A.I. and Adefemi, A., 2024. Blockchain in supply chain management: A review of efficiency, transparency, and innovation.

[53] Orieno, Omamode Henry, Chioma Ann Udeh, Osato Itohan Oriekhoe, Beryl Odonkor, and Ndubuisi Leonard Ndubuisi. "INNOVATIVE MANAGEMENT STRATEGIES IN CONTEMPORARY ORGANIZATIONS: A REVIEW: ANALYZING THE EVOLUTION AND IMPACT OF MODERN MANAGEMENT PRACTICES, WITH AN EMPHASIS ON LEADERSHIP, ORGANIZATIONAL CULTURE, AND CHANGE MANAGEMENT." *International Journal of Management & Entrepreneurship Research* 6, no. 1 (2024): 167-190.

[54] Osasona, F., Amoo, O.O., Atadoga, A., Abrahams, T.O., Farayola, O.A. and Ayinla, B.S., 2024. REVIEWING THE ETHICAL IMPLICATIONS OF AI IN DECISION MAKING PROCESSES. *International Journal of Management & Entrepreneurship Research*, *6*(2), pp.322-335.

[55] Reis, O., Eneh, N.E., Ehimuan, B., Anyanwu, A., Olorunsogo, T. and Abrahams, T.O., 2024. PRIVACY LAW CHALLENGES IN THE DIGITAL AGE: A GLOBAL REVIEW OF LEGISLATION AND ENFORCEMENT. *International Journal of Applied Research in Social Sciences*, *6*(1), pp.73-88.

[56] Surve, T. and Nguyen, T., 2024. Is Decentralized Control the Key for Digital Money?. In *Exploring Central Bank Digital Currencies: Concepts, Frameworks, Models, and Challenges* (pp. 42-58). IGI Global.

[57] Udeh, C.A., Orieno, O.H., Daraojimba, O.D., Ndubuisi, N.L. and Oriekhoe, O.I., 2024. BIG DATA ANALYTICS: A REVIEW OF ITS TRANSFORMATIVE ROLE IN MODERN BUSINESS INTELLIGENCE. *Computer Science & IT Research Journal*, *5*(1), pp.219-236.

[58] Usiagu, G.S., Adekoya, O.O., Okoli, C.E., Daudu, C.D., Ekemezie, I.O. and Ayorinde, O.B., 2024. LNG as a bridge fuel in the transition to renewable energy: A global perspective.

[59] Usiagu, G.S., Ayorinde, O.B., Okoli, C.E., Daudu, C.D., Adekoya, O.O. and Ekemezie, I.O., 2024. Environmental implications of LNG usage: A comparative review of policies in the USA and Africa.

[60] Yusoff, M.N.B. and Abd Ali, S.M., 2024. Bitcoin Layer Two Scaling Solutions: Lightening Payment Channels Network Comprehensive Review, Mechanisms, Challenges, Open Issues and Future Research Directions. *Iraqi Journal For Computer Science and Mathematics*, *5*(1), pp.25-59.