GSC Advanced Research and Reviews

eISSN: 2582-4597 CODEN (USA): GARRC2

Cross Ref DOI: 10.30574/gscarr

Journal homepage: https://gsconlinepress.com/journals/gscarr/

(REVIEW ARTICLE)

Leveraging blockchain for enhanced risk management: Reducing operational and transactional risks in banking systems

Chikezie Paul-Mikki Ewim [1,*], Chima Azubuike [2], Olajumoke Bolatito Ajani [3], Lawrence Damilare Oyeniyi [4] and Titilope Tosin Adewale [5]

[1] *Independent Researcher, Lagos, Nigeria.*
[2] *Guaranty Trust Bank (Nigeria) Limited.*
[3] *Newcross Exploration and Production Limited, Nigeria.*
[4] *Independent Researcher, UK.*
[5] *Independent Researcher, Canada.*

GSC Advanced Research and Reviews, 2022, 10(01), 182-188

Publication history: Received on 20 December 2021; revised on 22 January 2022; accepted on 24 January 2022

Article DOI: https://doi.org/10.30574/gscarr.2022.10.1.0031

Abstract

The banking sector faces significant challenges in managing operational and transactional risks, which can result in financial losses, inefficiencies, and reputational damage. With its unique attributes of decentralization, transparency, immutability, and advanced cryptographic security, blockchain technology offers a transformative solution to these challenges. This paper explores the role of blockchain in mitigating operational risks, such as human error, fraud, and system failures, through automation, enhanced auditability, and process accountability. It also examines how distributed ledger technology addresses transactional risks by improving payment security, minimizing settlement delays, and enhancing data integrity. The paper highlights the key benefits of blockchain adoption for risk management and provides recommendations for its effective implementation, including the need for regulatory adaptation, technological investment, and cross-sector collaboration. This analysis underscores the potential of blockchain to revolutionize banking operations and strengthen risk management frameworks in the financial sector.

Keywords: Blockchain Technology; Risk Management; Operational Risk; Distributed Ledger; Financial Security; Banking Systems

1. Introduction

Effective risk management is crucial in banking systems due to the complex and dynamic nature of the financial industry. Banks face many challenges, including operational inefficiencies, fraud, cybersecurity threats, and regulatory compliance (Lim, Woods, Humphrey, & Seow, 2017). These risks threaten the stability of individual financial institutions and can cascade into systemic crises, affecting entire economies. Thus, robust strategies for identifying, mitigating, and managing these risks are essential to ensure the security and resilience of banking operations (Onyiriuba, 2016).

Operational risks, often stemming from human errors, process failures, or technological vulnerabilities, are particularly critical. Transactional risks, on the other hand, involve issues such as payment fraud, reconciliation errors, and delays in clearing financial settlements (Xu, Pinedo, & Xue, 2017). Traditional risk management approaches have relied heavily on centralized systems and manual oversight, which, while effective to a degree, are increasingly insufficient in addressing the sophisticated challenges posed by today's digitalized financial ecosystems. This inadequacy calls for innovative solutions that leverage emerging technologies to enhance efficiency and security (Pandey, Singh, Gunasekaran, & Kaushik, 2020).

* Corresponding author: Chikezie Paul-Mikki Ewim.

Copyright © 2022 Author(s) retain the copyright of this article. This article is published under the terms of the Creative Commons Attribution Liscense 4.0.

Blockchain technology has emerged as a transformative tool for addressing these challenges. At its core, blockchain is a decentralized digital ledger that records transactions across a network of computers (Deshpande, Stewart, Lepetit, & Gunashekar, 2017). Its key features—transparency, immutability, and distributed consensus—make it a promising solution for mitigating risks in the banking sector. By enabling secure and tamper-proof record-keeping, blockchain eliminates the need for intermediaries, reduces the potential for human error, and strengthens the overall integrity of financial operations (Upadhyay, 2020).

This paper explores blockchain's role in enhancing risk management practices within banking systems. It will focus on two critical dimensions: mitigating operational and transactional risks. By examining the unique capabilities of blockchain, this discussion will highlight its potential to revolutionize risk management frameworks in financial institutions. Moreover, the paper will outline the practical benefits and limitations of integrating blockchain into banking systems while offering insights into its broader implications for the future of financial risk management.

2. Conceptual Foundations of Blockchain in Banking

Blockchain technology represents a significant innovation in digital infrastructure, potentially transforming various industries, particularly banking. At its core, blockchain is a distributed ledger that securely records transactions in a transparent, immutable, and decentralized manner. These attributes distinguish blockchain from traditional databases and centralized systems, offering unique banking operations and risk management advantages.

2.1. Decentralization

One of the most defining features of blockchain is decentralization. Unlike traditional centralized systems, where a single authority maintains and validates records, blockchain operates on a network of nodes that collectively verify and approve transactions. Each node contains a copy of the ledger, ensuring that no single point of failure can compromise the system. This structure enhances security and ensures continuous operation, even if some nodes are compromised (Viriyasitavat & Hoonsopon, 2019).

In banking, decentralization is particularly relevant for mitigating operational risks. For instance, centralized databases are often vulnerable to hacking, insider threats, or accidental data loss. A distributed system, however, reduces these vulnerabilities by spreading control and access across the network. This decentralization makes it difficult for malicious actors to manipulate records or disrupt operations, thereby strengthening the overall resilience of banking systems. (Essilfie-Conduah, 2019)

2.2. Immutability

Another key attribute of blockchain is immutability. Once a transaction is recorded on the blockchain and validated by the network, it becomes nearly impossible to alter or delete. This is achieved through cryptographic hashing, where each block in the chain contains a unique identifier linked to the previous block. Any attempt to modify a transaction would require altering all subsequent blocks, a computationally prohibitive task for even the most advanced systems (Politou, Casino, Alepis, & Patsakis, 2019).

In the context of risk management, immutability plays a critical role in ensuring data integrity and trustworthiness. Financial institutions often face challenges in maintaining accurate records due to errors, fraud, or unauthorized changes. Blockchain’s immutable ledger provides a tamper-proof record of all transactions, enabling banks to detect and prevent fraudulent activities more effectively. Additionally, this feature simplifies auditing and regulatory compliance by providing an unalterable history of financial activities (Jameaba, 2022).

2.3. Transparency

Transparency is another fundamental characteristic of blockchain. Transactions recorded on the blockchain are visible to all participants in the network, depending on the level of access granted. While public blockchains allow complete visibility, private and permissioned blockchains restrict access to authorized entities, balancing transparency with confidentiality (Benchoufi, Porcher, & Ravaud, 2018).

For banks, transparency fosters accountability and trust among stakeholders. It enables real-time monitoring of transactions, reducing the risk of undetected irregularities or discrepancies. This attribute is particularly valuable in multi-party transactions, such as cross-border payments or trade financing, where a lack of transparency can lead to disputes, delays, or financial losses. Blockchain’s ability to provide a single, shared source of truth ensures that all

parties have consistent and accurate information, minimizing operational inefficiencies and transactional risks (Sedlmeir, Lautenschlager, Fridgen, & Urbach, 2022).

2.4. Challenges of Traditional Risk Management Approaches

Traditional risk management approaches in banking rely heavily on centralized systems, manual oversight, and siloed operations. While these methods have been effective to an extent, they are increasingly inadequate in addressing the complexities of modern financial ecosystems.

One major limitation of centralized systems is their vulnerability to single points of failure. Whether due to cyberattacks, technical malfunctions, or natural disasters, the disruption of a central server can have catastrophic consequences for banking operations. Furthermore, centralized systems often involve lengthy reconciliation processes to ensure consistency across multiple parties, leading to delays and increased costs (Li, Shahidehpour, & Aminifar, 2017).

Manual oversight is another challenge, as it is prone to human error and inefficiency. Manual processes in high-volume environments like banking can result in data entry mistakes, missed anomalies, or delays in detecting fraudulent activities. These inefficiencies increase operational risks and undermine the overall effectiveness of risk management frameworks (Djenna, Harous, & Saidouni, 2021).

Siloed operations exacerbate these challenges by creating fragmented systems that hinder data sharing and collaboration. In traditional banking systems, different departments or entities often maintain separate databases, making achieving a unified view of risks difficult. This fragmentation limits the ability of institutions to respond proactively to emerging threats or coordinate effective risk mitigation strategies. Blockchain addresses these challenges by providing a decentralized, transparent, and immutable framework for managing data and transactions. Its ability to eliminate intermediaries, automate processes through smart contracts, and ensure real-time visibility makes it a game-changer for financial institutions seeking to enhance their risk management practices (Upadhyay, 2020).

3. Operational Risk Mitigation through Blockchain

Operational risks are among the most significant challenges faced by banking institutions. These risks arise from human error, internal fraud, system failures, and process inefficiencies, all of which can lead to substantial financial and reputational losses. Blockchain technology offers a transformative solution to these challenges by introducing mechanisms that enhance banking operations' accuracy, security, and accountability.

3.1. Reducing Human Error, Fraud, and System Failures

Human error is a pervasive issue in banking, often stemming from manual processes, inaccurate data entry, or miscommunication. Blockchain significantly mitigates these risks by automating data recording and validation through its decentralized ledger. Each transaction is verified and added to the ledger by the network, reducing reliance on individual oversight. This automated validation ensures consistency and accuracy across banking operations, minimizing the likelihood of errors (Bingzhang & Zirianov, 2021).

Fraud remains a persistent threat in the financial sector, often facilitated by weaknesses in centralized systems. Blockchain's cryptographic security and decentralized structure make it highly resistant to fraudulent activities. Transactions recorded on the blockchain are immutable, meaning they cannot be altered or deleted once validated (Zachariadis, Hileman, & Scott, 2019). This feature ensures that any attempt to manipulate data is easily detectable, thus deterring fraudulent practices. Additionally, the distributed nature of blockchain eliminates single points of failure, making it challenging for malicious actors to compromise the system (Yerram et al., 2021).

System failures, whether due to technical malfunctions or cyberattacks, can disrupt banking operations and result in significant losses. Blockchain enhances system resilience by distributing data across a network of nodes. In the event of a node failure, the system remains operational as other nodes maintain the ledger's integrity. This redundancy ensures continuous service availability and reduces the impact of system disruptions (Gajek, Lees, & Jansen, 2021).

3.2. Ensuring Compliance and Automation with Smart Contracts

Smart contracts, a key innovation within blockchain, play a pivotal role in mitigating operational risks. These self-executing contracts are encoded with predefined rules and conditions automatically enforced when specific criteria are met. Smart contracts eliminate the need for intermediaries and manual intervention, streamlining processes and reducing the potential for errors.

Smart contracts are particularly effective in ensuring compliance with regulatory and contractual obligations in banking. For instance, they can automate the enforcement of anti-money laundering requirements by verifying transactions against compliance criteria before approval. This automation reduces non-compliance risk and enhances operational efficiency by minimizing manual reviews (Turner, 2021).

Furthermore, smart contracts facilitate transparency and trust among stakeholders by providing a clear and auditable record of all actions executed. For example, a smart contract can automatically disburse funds, calculate interest, and schedule repayments based on agreed terms in loan processing. This reduces administrative overhead and ensures that all parties adhere to the contract's terms without requiring constant oversight (Staples et al., 2017).

The automation enabled by smart contracts also reduces delays and inefficiencies in banking processes. Traditional systems often involve multiple intermediaries, leading to time-consuming reconciliation and approval procedures. By automating these processes, smart contracts streamline operations, enhance accuracy, and minimize the risk of disputes or delays (Javaid, Haleem, Singh, Suman, & Khan, 2022).

3.3. Enhancing Process Auditability and Accountability

Auditability is a cornerstone of effective risk management, enabling banks to monitor and evaluate their operations for potential vulnerabilities. Blockchain's immutable ledger provides a reliable and tamper-proof record of all transactions, ensuring that every activity is traceable and verifiable. This level of transparency simplifies the auditing process, allowing regulators and internal auditors to easily identify discrepancies or anomalies.

The enhanced auditability of blockchain also improves accountability within banking institutions. With every transaction recorded on the ledger, individuals and entities involved in the process are held to higher responsibility standards. This reduces the risk of misconduct and ensures that any deviations from established procedures are promptly identified and addressed (Nimmagadda, 2021).

Moreover, blockchain's distributed nature ensures that all stakeholders have access to a consistent and accurate record of operations. This eliminates the challenges associated with reconciling multiple versions of data, which is common in traditional systems. By providing a single source of truth, blockchain fosters collaboration and trust among parties, further mitigating operational risks (Chitta, Yellepeddi, Thota, & Venkata, 2019).

In addition to these benefits, blockchain can support advanced risk management strategies through real-time monitoring and analytics. The technology enables banks to detect patterns and trends that indicate potential risks, allowing for proactive intervention. For instance, anomalies in transaction data can signal unauthorized activities, prompting immediate action to mitigate potential losses (Dutta, Choi, Somani, & Butala, 2020).

4. Transactional Risk Mitigation through Distributed Ledger Technology

Transactional risks in banking systems are pervasive, encompassing issues such as payment security vulnerabilities, settlement delays, reconciliation errors, and data breaches. Distributed ledger technology (DLT), the foundation of blockchain, offers a transformative approach to addressing these challenges. By leveraging its unique attributes, DLT enhances financial transactions' security, efficiency, and accuracy, creating a more robust framework for managing transactional risks.

4.1. Enhancing Payment Security and Reducing Settlement Delays

Payment security is critical to banking, as breaches can lead to significant financial losses and reputational damage. DLT enhances payment security by ensuring that all transactions are securely encrypted and recorded on a decentralized network. Unlike traditional systems, where sensitive financial information is often stored in centralized databases vulnerable to cyberattacks, DLT disperses data across multiple nodes. This decentralized architecture eliminates single points of failure, making it significantly more challenging for malicious actors to compromise the system (Wewege, Lee, & Thomsett, 2020).

The use of consensus mechanisms in DLT further strengthens payment security. Network participants verify transactions before being added to the ledger, ensuring that only legitimate transactions are recorded. This prevents unauthorized alterations and reduces the risk of fraud. Additionally, the immutability of DLT ensures that once a transaction is confirmed, it cannot be altered or deleted, providing an extra layer of security for payment processes (Hansen & Delak, 2022).

Settlement delays are another common transactional risk in traditional banking systems, often caused by the involvement of multiple intermediaries and outdated processes. DLT addresses this issue by enabling near-instantaneous settlement of transactions. With no need for intermediaries, transactions are processed directly between parties, significantly reducing the time required for settlement. This is particularly beneficial for cross-border payments, which traditionally take several days to clear. DLT minimizes delays and enhances customer satisfaction and operational efficiency by streamlining payment processes (Priem, 2020).

4.2. Minimizing Reconciliation Errors and Improving Data Integrity

Reconciliation errors occur when discrepancies arise between records held by different entities involved in a transaction. These errors often lead to financial losses, disputes, and inefficiencies in banking operations. DLT minimizes reconciliation errors by providing a consistent source of truth for all transaction data. Since every participant in the network has access to the same ledger, there is no need for time-consuming reconciliation processes (Roszkowska, 2021).

The transparency of DLT also plays a crucial role in improving data integrity. All transactions are recorded in real-time and are visible to authorized participants. This ensures that any discrepancies or anomalies can be quickly identified and resolved. The use of timestamps and cryptographic hashes further enhances data integrity by ensuring that each transaction is uniquely identifiable and securely linked to the preceding one.

In addition to reducing errors, DLT fosters trust among parties by eliminating the need for third-party verification. This is particularly valuable in financial ecosystems where multiple entities, such as banks, clearinghouses, and regulators, must collaborate. By providing a shared and tamper-proof ledger, DLT simplifies collaboration and reduces the potential for disputes (Javaid et al., 2022).

4.3. Cryptographic Security for Protecting Sensitive Financial Transactions

The protection of sensitive financial information is paramount in the digital age, where cyber threats are increasingly sophisticated. DLT employs advanced cryptographic techniques to secure financial transactions, ensuring that data remains confidential and protected from unauthorized access.

Public and private key encryption is a cornerstone of DLT's security framework. Each participant is assigned a pair of cryptographic keys: a public key, which is shared with the network, and a private key, which is kept confidential. Transactions are encrypted using the recipient's public key and can only be decrypted with their private key. This ensures that sensitive information remains secure throughout the transaction process (Astorga, Barcelo, Urbieta, & Jacob, 2022).

In addition to encryption, DLT employs digital signatures to verify the authenticity of transactions. Before a transaction is added to the ledger, the network verifies the sender's digital signature to ensure that it has not been tampered with. This mechanism prevents fraud and ensures non-repudiation, meaning that a party cannot deny involvement in a transaction once it has been recorded (Mandapuram, 2016).

The decentralized nature of DLT further enhances security by making it resistant to cyberattacks. Unlike centralized systems, where a breach can compromise the entire database, DLT stores data across a network of nodes. Even if one node is attacked, the integrity of the ledger remains intact, as the majority of nodes must agree on any changes. This makes DLT an ideal solution for protecting sensitive financial transactions in a high-risk environment (Farahani, Firouzi, & Luecking, 2021).

5. Conclusion

The adoption of blockchain technology in banking systems represents a transformative shift in managing risks, offering a more robust framework for addressing both operational and transactional vulnerabilities. By leveraging its key attributes—decentralization, transparency, immutability, and advanced cryptographic security—blockchain can significantly enhance the reliability and efficiency of financial operations. From minimizing human error and fraud to ensuring the integrity of sensitive data and expediting transactions, blockchain addresses critical shortcomings of traditional risk management practices.

Blockchain's ability to automate compliance through smart contracts, reduce reconciliation errors with distributed ledgers, and provide real-time auditability positions it as an indispensable tool in modern banking. These capabilities

mitigate risks and foster trust and efficiency, enabling financial institutions to better navigate the complexities of today's global economy.

For financial institutions to realize the full potential of blockchain, a strategic and phased approach to its implementation is essential. Below are key recommendations:

- Institutions must begin by assessing their specific risk management needs and identifying areas where blockchain can have the most significant impact. This involves thoroughly evaluating existing processes to pinpoint inefficiencies and vulnerabilities that blockchain can address.
- Blockchain implementation requires collaboration between banks, regulators, and technology providers. Financial institutions can ensure seamless integration of blockchain-based solutions across the ecosystem by establishing industry-wide standards and interoperable frameworks. Such collaboration also promotes trust and reduces resistance to adoption.
- Given the evolving nature of blockchain, regulatory frameworks must be adapted to balance innovation with risk control. Policymakers and financial institutions should work together to develop guidelines that support the secure deployment of blockchain solutions while ensuring compliance with anti-money laundering (AML) and data protection laws.
- Successful adoption of blockchain requires significant investment in digital infrastructure and technical expertise. Banks must ensure that their systems can handle the computational demands of blockchain, including secure storage of cryptographic keys and maintaining the scalability of distributed ledgers.
- For effective implementation, employees must have the knowledge and skills to operate within a blockchain-enabled environment. Institutions should provide training programs focusing on blockchain's technical and operational aspects to ensure a smooth transition.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Astorga, J., Barcelo, M., Urbieta, A., & Jacob, E. (2022). Revisiting the feasibility of public key cryptography in light of iiot communications. *Sensors, 22*(7), 2561.

[2] Benchoufi, M., Porcher, R., & Ravaud, P. (2018). Blockchain protocols in clinical trials: Transparency and traceability of consent. *F1000Research, 6*, 66.

[3] Bingzhang, L., & Zirianov, V. (2021). *Blockchain in agricultural supply chain management.* Paper presented at the E3S Web of Conferences.

[4] Chitta, S., Yellepeddi, S. M., Thota, S., & Venkata, A. K. P. (2019). Decentralized Finance (DeFi): A Comprehensive Study of Protocols and Applications. *Distributed Learning and Broad Applications in Scientific Research, 5*, 124-145.

[5] Deshpande, A., Stewart, K., Lepetit, L., & Gunashekar, S. (2017). Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards. *Overview report The British Standards Institution (BSI), 40*(40), 1-34.

[6] Djenna, A., Harous, S., & Saidouni, D. E. (2021). Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure. *Applied Sciences, 11*(10), 4580.

[7] Dutta, P., Choi, T.-M., Somani, S., & Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. *Transportation research part e: Logistics and transportation review, 142*, 102067.

[8] Essilfie-Conduah, N. (2019). *A systems analysis of insider data exfiltration: a decentralized framework for disincentivizing and auditing data exfiltration.* Massachusetts Institute of Technology,

[9] Farahani, B., Firouzi, F., & Luecking, M. (2021). The convergence of IoT and distributed ledger technologies (DLT): Opportunities, challenges, and solutions. *Journal of Network and Computer Applications, 177*, 102936.

[10] Gajek, S., Lees, M., & Jansen, C. (2021). IIoT and cyber-resilience: Could blockchain have thwarted the Stuxnet attack? *AI & society, 36*(3), 725-735.

[11] Hansen, T., & Delak, K. (2022). Security considerations for a central bank digital currency.

[12] Jameaba, M.-S. (2022). Digitalization, Emerging Technologies, and Financial Stability: Challenges and Opportunities for the Indonesian Banking Industry and Beyond. *DOI: https://doi. org/10.32388/CSTTYQ, 2*.

[13] Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Khan, S. (2022). A review of Blockchain Technology applications for financial services. *BenchCouncil Transactions on Benchmarks, Standards and Evaluations, 2*(3), 100073.

[14] Li, Z., Shahidehpour, M., & Aminifar, F. (2017). Cybersecurity in distributed power systems. *Proceedings of the IEEE, 105*(7), 1367-1388.

[15] Lim, C. Y., Woods, M., Humphrey, C., & Seow, J. L. (2017). The paradoxes of risk management in the banking sector. *The British Accounting Review, 49*(1), 75-90.

[16] Mandapuram, M. (2016). Applications of Blockchain and Distributed Ledger Technology (DLT) in Commercial Settings. *Asian Accounting and Auditing Advancement, 7*(1), 50-57.

[17] Nimmagadda, V. S. P. (2021). Artificial Intelligence and Blockchain Integration for Enhanced Security in Insurance: Techniques, Models, and Real-World Applications. *African Journal of Artificial Intelligence and Sustainable Development, 1*(2), 187-224.

[18] Onyiriuba, L. (2016). *Bank risk management in developing economies: Addressing the unique challenges of domestic banks*: Academic Press.

[19] Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing, 13*(1), 103-128.

[20] Politou, E., Casino, F., Alepis, E., & Patsakis, C. (2019). Blockchain mutability: Challenges and proposed solutions. *IEEE Transactions on Emerging Topics in Computing, 9*(4), 1972-1986.

[21] Priem, R. (2020). Distributed ledger technology for securities clearing and settlement: benefits, risks, and regulatory implications. *Financial Innovation, 6*(1), 11.

[22] Roszkowska, P. (2021). Fintech in financial reporting and audit for fraud prevention and safeguarding equity investments. *Journal of Accounting & Organizational Change, 17*(2), 164-196.

[23] Sedlmeir, J., Lautenschlager, J., Fridgen, G., & Urbach, N. (2022). The transparency challenge of blockchain in organizations. *Electronic Markets, 32*(3), 1779-1794.

[24] Staples, M., Chen, S., Falamaki, S., Ponomarev, A., Rimba, P., Tran, A., . . . Zhu, J. (2017). Risks and opportunities for systems using blockchain and smart contracts. Data61. *CSIRO), Sydney*.

[25] Turner, B. (2021). The smarts of'smart contracts': Risk management capabilities and applications of self-executing agreements. *ANU Journal of Law and Technology, 2*(1), 89-117.

[26] Upadhyay, N. (2020). Demystifying blockchain: A critical analysis of challenges, applications and opportunities. *International Journal of Information Management, 54*, 102120.

[27] Viriyasitavat, W., & Hoonsopon, D. (2019). Blockchain characteristics and consensus in modern business processes. *Journal of Industrial Information Integration, 13*, 32-39.

[28] Wewege, L., Lee, J., & Thomsett, M. C. (2020). Disruptions and digital banking trends. *Journal of Applied Finance and Banking, 10*(6), 15-56.

[29] Xu, Y., Pinedo, M., & Xue, M. (2017). Operational risk in financial services: A review and new research opportunities. *Production and Operations Management, 26*(3), 426-445.

[30] Yerram, S. R., Goda, D. R., Mahadasa, R., Mallipeddi, S. R., Varghese, A., Ande, J., . . . Dekkati, S. (2021). The role of blockchain technology in enhancing financial security amidst digital transformation. *Asian Bus. Rev, 11*(3), 125-134.

[31] Zachariadis, M., Hileman, G., & Scott, S. V. (2019). Governance and control in distributed ledgers: Understanding the challenges facing blockchain technology in financial services. *Information and organization, 29*(2), 105-117.