Bank and Policy | ISSN Print: 2790-1041 | ISSN Online: 2790-2366

IMCRA

Research Article, 2026,1,9

The Role of Blockchain Technology in Strengthening Security, Transparency, and Trust in Banking Transactions: A Conceptual and Empirical Review of Distributed Ledger Applications in Modern Financial Systems

Author (s): Vanshika Thakur[1]; Gosala Raju[2]

1. *Research Scholar, Guru Ghasidas Vishwavidyalaya, Bilaspur, Chhattisgarh, vanshika.180899@gmail.com*
2. *Dr. Assistant Professor, Guru Ghasidas Vishwavidyalaya, Bilaspur, Chhattisgarh, gosala.raju39@gmail.com.*

Citation in APA 7: Thakur, V., & Raju, G. (2026). The role of blockchain technology in strengthening security, transparency, and trust in banking transactions: A conceptual and empirical review of distributed ledger applications in modern financial systems.. *Bank and Policy*, 6(1), 107–119.

Received: 08.10.2025 **Accepted**: 22.01.2026 https://doi.org/10.56334/bpj/6.1.9

Keywords: Blockchain Technology; Banking Transactions; Security; Transparency; Distributed Ledger Technology; Financial Innovation.

Abstract

As banking has rapidly digitised around the world, many new transaction systems must be secure, transparent and trusted. Traditional banking is often challenged by data breaches, fraud, opaqueness and inefficiencies in verifying and reconciling transactions, as a result of banking's Centralised infrastructure. Blockchain technology offers a new way of developing more secure and transparent ways of carrying out banking transactions through Distributed Ledger Technology (DLT). This paper uses a secondary data research methodology to analyse the Security & Transparency benefits of Blockchain Technology within the banking sector. By using peer-reviewed journal articles, reports produced by international financial institutions and examples of Blockchain Technology used by industry participants, the paper evaluates how the core characteristics (e.g., decentralised, immutable, cryptographically secure, and consensus mechanisms) of Blockchain Technology increase the security of banking transactions while simultaneously improving transparency within all areas of a bank's operations. In addition, this paper examines how Blockchain Technology can be used in Payment Systems, Settlement Systems, Auditing and Complying with Financial Regulations and identifies the obstacles to implementing Blockchain Technology: scalability, regulatory compliance, and compatibly with legacy systems. The results suggest there is tremendous opportunity to change banking transaction systems with Blockchain Technology if there are appropriate regulatory structures and wise institutional preparation.

1. Introduction

The banking sector is an essential component of ensuring the stability of the economy by providing services for payments, savings, creating credit, and being a financial intermediary in general. As the banking industry becomes more dependent on digital platforms, concerns about transaction security, data integrity, fraud, and lack of transparency have become a significant issue. The centralized nature of banking systems makes them especially susceptible to cyberattacks, unauthorized manipulation of data, and asymmetry of information, leading to a breakdown of trust between customers and regulators.

There has been increasing interest in Blockchain Technology as a form of Digital Technology that can solve this problem. Blockchain's original introduction as the underlying technology of Bitcoin (Nakamoto, 2008) has since evolved into a multi-use platform for multiple industries - Banking/Finance included. Blockchain's decentralized model allows for immutable record retention and blockchain utilizes cryptographic principles to provide security. This proves that Blockchain is well positioned to improve trust, security, and transparency in Banking/Financial Transactions.

Recently, several Banks/Financial Institutions are examining Blockchain Technology as a potential avenue for the production of payments; settlement systems; trade finance; audits; and compliance with Government and Regulatory Agencies. Emerging and Developed Markets are beginning to understand Blockchain as a means to mitigate fraud; increase transparency and facilitate greater Operational Efficiency. Therefore, this study of the Literature and Secondary Data will assist in developing a comprehensive overview on the ways in which Blockchain Technology can increase trust, security and transparency within Banking Transactions; and the potential of Blockchain to help improve Security and Transparency of Financial Transactions.

2. Conceptual and Theoretical Framework

2.1 Blockchain Technology as a Financial Innovation

Blockchain is an electronic ledger that records all financial transactions across many different computers in a secure and transparent way that cannot be altered by any person. Each record of transaction on the blockchain gets bundled into a block that is encrypted and linked with the previous one; ultimately, this creates an endless chain of blocks (Nakamoto, 2008). Whereas traditional centralized databases require a single point of control, blockchain is built on consensus among the entire network of participants to authenticate transaction.

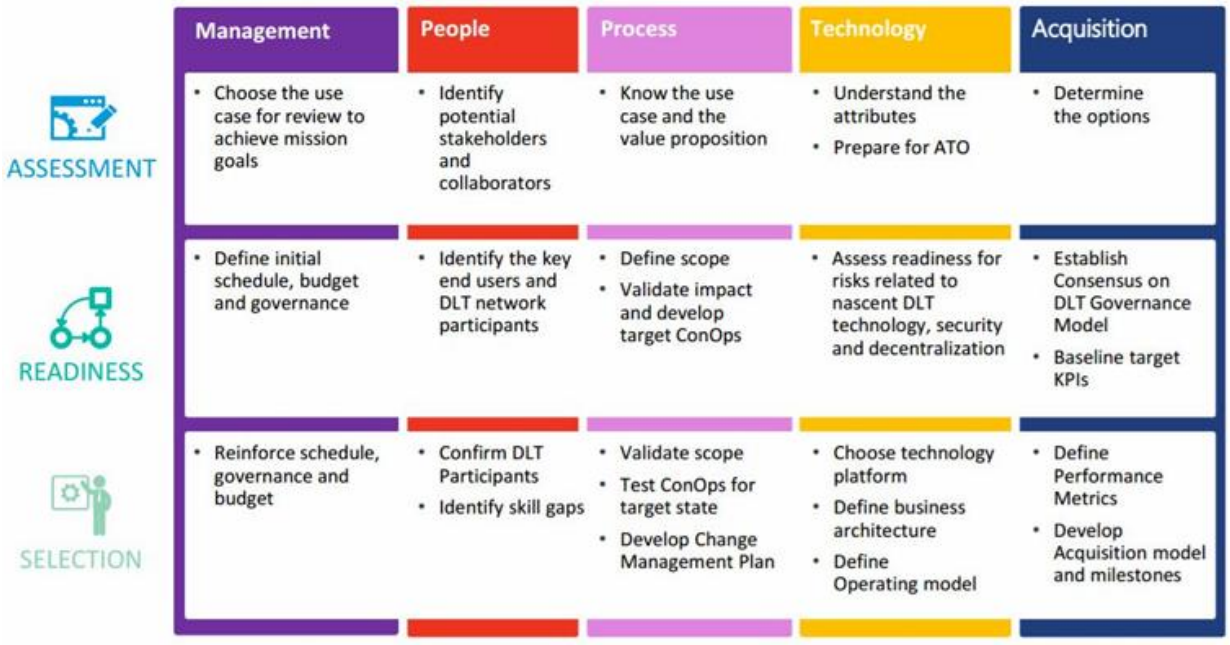

Figure 1: Blockchain Adoption Framework in Banking: Assessment, Readiness, and Selection Stages

Source: (Berryhill et al., 2018)

2.2 Theoretical Foundations

The Financial Intermediation Theory provides the basis for this study; according to Beck et al. (2016), financial institutions facilitate transaction cost reduction, risk management, and information asymmetry remediation. Blockchain technology supports all three items by removing intermediary reliance for trust, automating trust with technology, and creating even levels of interchangeability through shared ledgers.

According to Agency Theory, there will always be situations in which stakeholders will disagree over how best to use a resource based upon their differing viewpoints. With the ability of stakeholders to confirm transactions through visible and unalterable records, agencies can more effectively deter opportunistic behaviour (Vives, 2019).

The Technology Acceptance and Innovation Diffusion Framework provides insights regarding the nature of Blockchain adoption in the Banking industry through perception of tangible benefits associated with Blockchain Technology as opposed to that of traditional systems as demonstrated through increased security and perceived usefulness (Gomber et al., 2017).

3. Review of Literature

The increasing involvement of the blockchain industry has generated an abundance of scholarly and policy-oriented literature on how the blockchain could affect the banking and finance industries. These researchers tend to stress that by using blockchain technology, banks and financial service providers may enhance security and efficiency in transactions while improving the way they provide financial services. This paper provides an overview of key theoretical frameworks and empirical findings that help to develop our knowledge of the ways in which blockchain could be used to further support the development of the banking and financial services industries, focuses specifically on the areas of security and transparency, and offers insights into existing research challenges and gaps in the available literature.

3.1 Blockchain Technology and Security in Banking Transactions

Numerous studies have indicated that decentralisation of the transactional process, using cryptographic encrypting techniques and implementing various validation methods for consensus, allow Blockchain Technology to provide transaction security through increased security and transparency (Nakamoto, 2008). The original article emphasises that distributed ledgers remove barriers to double-spending and unauthorised modifications of transaction records. This is achieved by the decentralisation of the control of all transaction records and eliminating the reliance on a single central entity for the validation of transactions. Distributed ledger Technology is widely considered the best means to mitigate the risk of fraud and cyber threats in the Banking sector.

As noted in Beck et al. (2016), Blockchain Technology has improved the security of the financial sector by reducing the occurrence of information asymmetries and decreasing the opportunity for opportunistic behaviours. The authors continue to explain that through the application of a distributed ledger, it is almost impossible to alter records of transactions without being detected. Consequently, the integrity and reliability of the data created and maintained by the distributed ledger will be significantly enhanced. Vives (2019) confirms this argument by indicating that the implementation of blockchain enables the reduction of systemic risk through the removal of common points of failure created by centralised databases in the banking sector.

Empirical research has further verified the ability of blockchain technologies to improve security in banking. Research conducted by Berryhill et al. (2018) suggests that Banks and their customers use the Blockchain for Payments and Financial Settlement, thereby increasing the number of nodes in which transaction data can be stored and decreasing the potential for third-party access; therefore, decreasing the risk of data breaches. In addition, Dewi et al. (2025) have researched ways to prevent internal fraud and the alteration of financial data by using the appropriate applications of cryptographic hashing and by creating an immutable record.

3.2 Blockchain and Transparency in Financial Transactions

Additionally, the concept of transparency is another area that has been extensively studied and documented in the literature related to Blockchain. Many of the traditional methods of banking have upwards of multiple layers of intermediaries involved when moving through multiple institutions and geographies to facilitate the transaction, therefore there is often a lack of visibility into the transaction process. One of the primary features of Blockchain is that all authorised participants have access to the same live record of transactions (BIS, 2018).

Numerous scholarly articles have documented how blockchain's immutable audit trails will enhance accountability as well as provide traceability on banking transactions. Al Husseini (2025) states that blockchains allow banks to maintain a ledger

of transactions which has permanent and auditable records that can be verified. This will decrease the number of man-hours needed to reconcile transactions, and therefore increase the level of compliance with regulatory reporting requirements.

Sahay et al. (2020) asserts that the transparency of information made available through Blockchain is increasing the level of trust in between banks, customers, and regulators. These authors further state that allowing all parties involved in the transaction to access verifiable data of all transactions in real time will lessen the incidence of disputes concerning transaction integrity and increase confidence in the validity of financial systems as well as encourage use of those systems by consumers. Philippon (2016) states that allowing individuals and businesses to have access to a verifiable record of their transaction information creates lower levels of monitoring costs and an overall increase in the efficiency of the financial system.

3.3 Blockchain Applications in Banking Operations

In addition, the academic literature has examined how blockchain can be applied in banking. One area that has received the greatest attention to date is that of cross-border payments. Historically, international payment systems are known for their high costs, lengthy delays in settling transactions, and lack of transparency.

Blockchain has great potential in the trade finance and interbank settling space by vastly improving the efficiency of document verification, minimising fraud and also expediting the process of settling transactions by allowing all the participating banks to access a shared record of transactions executed within that system (Beck et al., 2016). Additionally, Gomber et al. (2017) state that Smart Contracts, which can be defined as contracts that execute automatically when certain conditions are met, will dramatically change how contracts are completed and enforced because this will eliminate human errors and reduce operational risks.

Some authors also suggest that the number of banks and other financial institutions using Blockchain for their internal audit and compliance functions is increasing. For example, Vives (2019) highlights that the ability to use blockchain as a tool for the internal audit process provides for continual monitoring as opposed to periodic monitoring of samples which increases an institution's capability for identifying potential risks as well as meeting regulatory compliance requirements.

3.4 Regulatory and Institutional Perspectives

While the potential impact of Blockchain in banking has been documented extensively, literature demonstrates that there are many regulatory and institutional barriers that will limit or inhibit the application of Blockchain technology to banks. Douglas W. Arner (2017) identifies the lagging regulatory frameworks as a large factor in creating a climate of uncertainty surrounding the consideration of Blockchain solutions by banks. Furthermore, most countries still have not addressed some of the major issues surrounding Blockchain, including: data privacy laws, jurisdictional boundaries, and the legal recognition of Blockchain-generated records.

The IMF (2019) issued a warning in 2019 that although Blockchain Technology is designed to improve Transparency, Blockchain also has the potential of creating problems by creating excessive levels of Openness that conflict with the know-your-customer regulations. As a result of the problems, the Banking Sector is beginning to focus more on Hybrid or Permissioned Models that will allow them to maintain a balance between Transparency and Privacy and also comply with Regulatory Activities.

Many Researchers also point to Institutional Barriers such as High Implementation Costs, Integration with Legacy Systems, and Skill Gaps as significant challenges facing the Banking Industry today (Berryhill et al., 2018). These obstacles may present challenges regarding the scalability and effectiveness of Blockchain Technology, particularly within Emerging Economies that do not possess a strong Technological Infrastructure.

3.5 Research Gaps

While there is a wealth of research available regarding the potential of Blockchain Technology to increase Security and Transparency in Banking Transactions, there remain many gaps in the Research. The First Gap is that the majority of Research has focused on separate use Cases and/or Theoretical Usage Methods for increasing Security and Transparency without documenting a Combination of both Security improvements and Transparency improvements resulting from the use of Blockchain Technology within a single integrated Banking Framework. A second gap is the lack of Empirical Evidence concerning the use and acceptance of Blockchain Technology in Emerging Economies as the bulk of Studies are limited to Developed Economies.

In addition, comprehensive studies based on secondary sources that include all academic, policy, and industry perspectives of blockchain adoption in banks do not currently exist. More specifically, these gaps must be addressed to determine how

blockchain can be used effectively to strengthen secure and transparent banking systems within the diverse contexts of different institutions.

4. Research Methodology

4.1 Research Design

The use of secondary data sources for this study is appropriate given that the adoption of blockchain by banks has been evolving rapidly, and there are numerous existing research articles, government documents, and industry reports providing detailed information regarding the use, advantages, and challenges of blockchain technology in bank (Johnston, 2014).

Derogative and Analytical Research Methodologies Allow for Systematic Documentation of Current Trends, Applications, and Results Associated with Blockchain. Analytical Research Methodologies, however, Allow for Evaluation of Any Existing Empirical Evidence, in all cases across Various Contexts for the Purpose of Synthesizing or Evaluating their Value as a Research Reference Resource In FinTech Research, Where the Availability of Empirical Primary Data is Limited by the Regulatory Environment and Access to Institutional Banking Systems, Derogatory Research Methodologies are Commonly Utilized (Sahay et al., 2020).

4.2 Sources of Data

All data used in this study were collected from secondary data sources and were restricted to those sources that were credible, publicly available, and academic in nature. all sources of evidence utilized in this study (Saunders et al., 2023) are listed below:

- Peer-reviewed Journal Articles Indexed in Scopus, Science Direct, or other Scientific Journals
- Reports Issued by International Financial Institutions, i.e. Bank of International Settlements (BIS), International Monetary Fund (IMF), World Bank, and Organisation for Economic Co-operation and Development (OECD)
- Technical Reports/White Papers Published by National Financial Regulatory Agencies and/or Central Banks
- Industry-Sponsored Reports from Financial Technology Consulting Firms and/or Research Organisations

5. Role of Blockchain in Enhancing Security and Transparency in Banking Transactions

a) The effect of Blockchain on banking has been vast. It offers different options to the same issues around security, integrity of data, and transparency that banks have encountered for years. In contrast to traditional banking methods where many banks rely upon a number of different middlemen and use a central database, Blockchain allows banks to remove these centralization points, reducing numerous security risks. Some of these security risks include: The fact that one central server may be compromised (the "single-point-of-failure"), the fact that unauthorized people can alter transaction data, the long time required to reconcile transactions and a general lack of knowledge about where money always exists. **Enhancing Transaction Security**

More than just improving security, the primary benefit of Blockchain when it comes to banking transactions is that banks can implement innovative ways to protect their sensitive transaction data through the use of advanced cryptography regarding the encrypting and securing of transaction data. All transactions created using blockchain are cryptographically secured, linked to prior transactions using cryptographic hashes, and stored as unchangeable digital records in a permanent ledger. After verifying and adding transactions to the ledger, changes cannot be made, thus eliminating any chance of fraudulent activity, unauthorized access to funds, or altered data.

Decentralization increases the degree of security by eliminating the dependence on a single repository or central authority. Conventional banks have centralized records that can make them attractive targets for cyberattacks; when one of these centralized records is compromised, considerable amounts of personal and sensitive data may also be compromised. By using blockchain technology to distribute all transaction information across several nodes of a network, it will be very difficult to hack any single node of the network and compromise a large number of transaction records at the same time. In order to make a malicious change to the data in the blockchain, the malicious person would have to control a majority (more than 50 percent) of all nodes within the entire network (which is virtually impossible when the network is built; it is highly unlikely that any single individual or group will be able to control that many nodes).

Blockchain security is further enhanced with the use of consensus models such as Proof-Of-Work (PoW), Proof-Of-Stake (PoS), and permissioned consensus models, which are used widely by banks and other financial institutions to verify transactions for the public's benefit. These consensus models help ensure that only authenticated and approved transactions

are entered into the blockchain, which reduces the chance of fraud or the addition of duplicate transactions by means of a shared ledger.

b) Improving Transparency and Traceability

Blockchain technology offers different levels of visibility into financial transactions compared to traditional financial reporting systems, which can only provide information for a limited period of time. The transparency offered throughout the life cycle of every transaction enables the participants involved in that lifecycle (i.e., the bank, the auditor, the regulator, etc.) to have access to the same information. As a result, the lending institutions involved in the transaction have equal access to this same data and can use this information to determine how they should treat the transaction for the purposes of determining compliance with regulatory requirements.

Each transaction entered into the blockchain is created with a timestamp, an audit trail, and a digital signature that is unique to the transaction. Thus, the party performing the audit can look at the blockchain and determine the complete history of the transaction, such as who performed the transaction, how much was transacted, and when the transaction happened (date/time). Consequently, because auditing capabilities for the blockchain are superior to those of banks, reliance on bank-generated reports to confirm transactions is unnecessary.

Instead of using the conventional ways of banking, which consist of understanding whether or not to have money in a bank account before reconciling the two accounts by usually comparing them to determine if they are correct, banks that use blockchain will have automated audits and the ability to audit continuously. The transparency of the blockchain will reduce the costs associated with resolving disputes and reconciling accounts between banks (in particular between banks in different countries), as both banks can see the same validated data on the blockchain, which helps to decrease discrepancies and increase the efficiency of operations by speeding up the time it takes to settle a transaction.

c) Fraud Prevention and Risk Mitigation

Bank businesses will still need protection from different types of fraud including, among other types of fraud, payment fraud, identity theft, and unauthorized changes to bank records. The immutability of the blockchain technology, as well as its ability to provide transparency, allows banks to easily detect and stop fraudulent transactions and identity theft. Because once a transaction has been recorded on the blockchain, it creates an identifiable trace of that transaction on the ledger. Therefore, identifying fraud and identity theft will be done by finding anomalies on the blockchain ledger.

Smart Contracts are a type of computer program that gets executed automatically based on the occurrence of a particular event or series of events, as determined by the rules set out in its code. For Banks and other financial institutions, Smart Contracts can automate the entire process of loan disbursement, finance for international trade, and settlement. A Smart Contract creates a legal agreement so the agreed-upon business actions can occur under a pre-defined set of conditions agreed upon by both parties. As Smart Contracts reduce the involvement of humans in executing and completing business transactions, there will be less chance for an error to occur when executing these transactions, and therefore the risk of fraud or corruption will decrease significantly.

d) Strengthening Data Integrity and Trust

Areas of Banking Operations in which keeping Data Integrity has the greatest importance include: (i) Payments (ii) Customer Records (iii) Compliance Reporting. Using Blockchain will enable Financial Institutions to maintain complete and accurate records of all transactions processed by an institution throughout its network of participants, thus providing the institution's customers with the confidence that their Transaction Records are accurate and will not be altered, nullified or destroyed without the customer's authorization.

As such, when customers use Blockchain based Banking services, they will be more confident in using the Bank's Digital Financial Services, as well as the potential for improved Reputation for Banks due to increased Trust, reduced Compliance Risks, and Improved Customer Relationships.

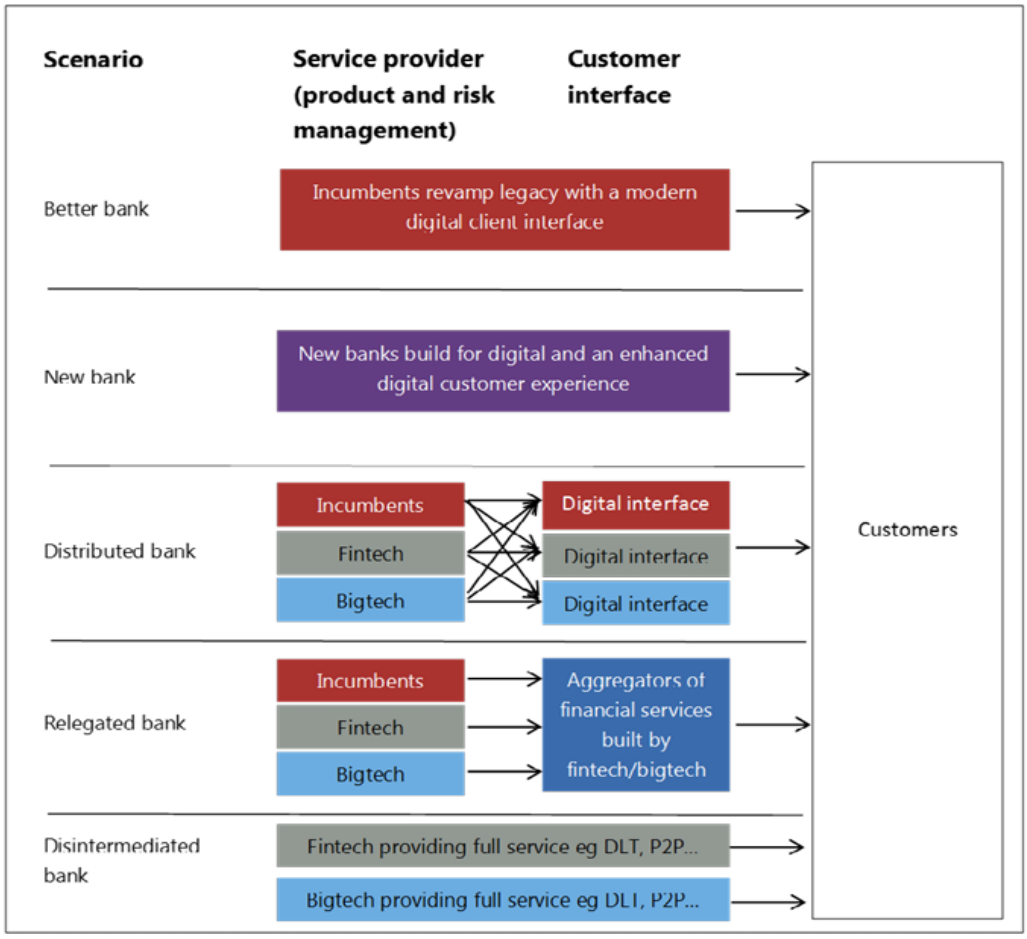

Figure 2: Evolution of Banking Models in the Digital and Distributed Ledger Technology

Source: (BIS, 2018)

e) Applications in Banking Transactions

Banks are using blockchain technology for many of their banking functions including: Cross-Border Payments, Interbank Settlement, Trade Finance, Identity Verification and Record Management. Banks are utilizing blockchain to provide customers with real-time access to payment services and transaction histories which increases efficiency and satisfaction through immediate access. As banks continue to embrace blockchain and develop business-to-business relationships using this innovative technology they will face many of the same challenges that all businesses face when implementing new technologies.

Some of the key challenges faced by banks when adopting blockchain technology include: lack of regulatory clarity surrounding various aspects of the blockchain ecosystem, adoption of blockchain by smaller financial service providers; scalability constraints caused by the current infrastructure on which banks operate; and the high upfront costs associated with the deployment of blockchain technology. These challenges represent major roadblocks to further blockchain adoption. Solutions are being developed for the challenges faced by banks as the use of blockchain evolves which should help to reduce barriers to entry and increase confidence in the bank's capabilities as a participant in the ever-changing digital financial world.

6. Challenges and Risks of Blockchain Adoption in Banking Transactions

Blockchain technology has considerable potential to increase both the security of banking transactions as well as transparency in banking transactions; however, multiple challenges and risks are associated with the implementation of blockchain across banks. A variety of technological, regulatory, operational and institutional challenges lead to the difficulty of using blockchain in many emerging and developing economies. If left unaddressed these challenges will affect the way banks will be able to scale blockchain technology, how efficient and scalable it will be and how sustainable it will be.

- **Technological and Scalability Challenges**

The scalability of blockchain technologies for banks is one of the most significant obstacles to blockchain implementation. The transaction processing speed and network throughput limitations of public blockchain networks present many challenges for banks, especially those with millions of transactions processed every day. As banks begin to process their transaction volumes digitally, the likelihood that there will be significant delays and increased transaction fees due to the fact that the blockchain network is unable to handle the increased transaction volume becomes a real possibility for banks.

Furthermore, the operation of a large distributed ledger will require a considerable amount of computing and storage resources. Another significant operational challenge for banks is the complexity of integrating blockchain technology into their existing core banking systems and Legacy infrastructure. Most banks have been using systems that are many years old; thus, they cannot easily connect to a decentralized platform. Therefore, implementing blockchain technology in the banking industry will be much more difficult because legacy systems will not integrate easily with the new technology being used within decentralised platforms.

- **Cybersecurity and Operational Risks**

The technology of block chain is a fundamentally secure form of technology; however, it is not without risk in terms of cybersecurity. there are vulnerabilities that can arise due to poorly designed smart contracts, access to cryptographic keys without proper authorization and issues with the applications and interfaces surrounding them. In addition, there are also considerable risks to the security of block chain systems due to phishing attacks, ransomware, and insider threats namely for users who are inexperienced with cybersecurity best practices.

Banks are increasingly faced with additional operational risks due to their use of distributed networks to enable transaction processing via third party block chain service providers. The risk of operational failure is then compounded by the problems that will occur from software defects and other forms of operational failure (causing service disruption) and therefore increasing their chances of experiencing financial loss due to reputational damage.

- **Regulatory and Legal Uncertainty**

The lack of clear regulations as they relate to use of blockchain technology in the financial sector is a major roadblock to the widespread adoption of blockchain in bank operations. Current banking regulation has traditionally been created with decentralised institutions, such as banks, and intermediaries in mind, and does not explicitly address the status under law for the transfer of money between bitcoin wallet(s) (where lots of crypto is stored digitally), smart contracts, or other types of digital assets. Also, many essential items still require clarity by regulators – (1) ownership/possession of the data that was transmitted, (2) what jurisdiction is responsible for resolving disputes.

When conducting International transactions using blockchain, banks must follow many of the same rules that they do with traditional payments when they send payments across borders. This creates additional compliance hurdles and increases the potential risk of being subjected to multiple regulations, conflicting regulatory requirements from different countries, and creating more uncertainty regarding compliance. The regulatory variances between countries also create confusion and uncertainty, which leads to fewer banks utilising blockchain for International payment volume.

- **Data Privacy and Confidentiality Concerns**

Although blockchain has several advantages over traditional banking methods due to its high level of transparency, it also presents significant obstacles to ensuring customer and transaction data privacy and confidentiality. Transaction banking data includes a great deal of sensitive customer and financial information, so it is vital that banks maintain this information privately and securely, as mandated by various laws governing data protection, such as the General Data Protection Regulation in Europe. The same challenge exists with both public and permissionless blockchains due to their ability to fully disclose transaction details, creating issues for banks covered under these regulations.

The use of permissioned blockchains and encryption technology may reduce the full disclosure of transaction details but still presents substantial technical difficulties in properly achieving privacy compliance for banks that wish to deploy blockchain technology according to applicable regulations. A key challenge for banks implementing blockchain technologies under compliance with Data Protection Laws is effectively fulfilling both the regulatory requirement to provide public transparency and the obligation to maintain private confidentiality of customer information.

- **Skill Gaps and Organizational Resistance**

Presently, a significant number of banks are experiencing a lack of qualified staff and/or analytical expertise to successfully implement blockchain technology. This shortage of qualified personnel contributes to the ongoing slow adoption of blockchain and the increased reliance on outside technology providers.

Another challenge to the successful implementation of blockchain technology will be the changing organizational structures that will be caused by the movement from centralised to decentralised systems. The shift to decentralisation will require changes to both the corporate culture and structure. Potentially, employees and management may oppose such a transition, as there is an inherent lack of understanding (uncertainty) regarding the perceived risks associated with blockchain technology. The combination of organisational resistance and lack of technical knowledge may create barriers to the successful integration of blockchain technology into many banks' existing operations.

- **Cost and Economic Viability**

Implementing blockchain technology can require a significant investment in technology infrastructure, system integration, security, and training staff for banks, particularly small and mid-sized banks, so the initial cost could be greater than the short-term benefits therefore the financial burden of adopting blockchain technology could prevent banks from making any commitment to it. Additionally, the lack of clarity regarding return on investment (ROI) and the long implementation period can also dissuade banks from committing any of their financial resources to blockchain solutions.

7. Policy and Managerial Implications

For financial institutions, regulators, and policy makers, the use of blockchain technology for banking transactions can have a significant impact. To achieve the desired benefits of enhanced security, transparency, and reduced reliance on third parties due to the use of block chain, all stakeholders at the local and national levels need to take coordinated action at both the policy and institutional levels to ensure that blockchain solutions are effectively governed and regulated, and successfully implemented.

Policy Implications

From a regulatory standpoint, there must be an appropriate and flexible regulation/infrastructure to support financial innovations utilizing blockchain technology in a manner that is technology-neutral. Current banking regulations were designed with the assumption that all systems would be centralized. Therefore, current banking regulations do not address decentralized/distributed technologies like blockchain. Furthermore, policymakers must determine the classification of blockchain transactions, smart contracts, and digital records as it relates to financial regulatory policy, which will reduce doubt about these technologies and increase confidence on the part of institutions.

Regulatory sandboxes can be instrumental in encouraging the responsible use of blockchain technology. They create an environment in which banks and fintechs can create new applications that use blockchain technology while being subject to regulatory oversight. By creating a safe environment for banks and fintechs to test and evaluate their blockchain applications, regulatory sandboxes provide an opportunity for regulators to identify potential risks associated with these applications and to test compliance processes while supporting innovation without jeopardizing the entire financial market. Regulators will have a clearer understanding of how the technology they are reviewing works and how to develop a regulatory response based on evidence from the sandbox process.

Industrial Standards should be established that specify how blockchain technology can be used, including how to secure data, provide access control to data, encrypt data stored on the blockchain, and provide a way for auditors to verify compliance and reasonable assurance of compliance with standards of confidentiality and transparency. A high degree of harmonization and mutual recognition of data protection standards will become increasingly important as cross-border blockchain transactions increase.

Digital infrastructure and capacity building are a second major policy priority. Therefore governments should invest in the establishment of secure digital networks, interoperable platforms, and standardised protocols that provide for the seamless incorporation of Blockchain within the banking sector, so that financial institutions can connect to One Another, without having to worry about compatibility issues.

Managerial Implications

A manager's ability to manage change and gauge an organisation's preparedness to implement new technology is also paramount. Given that blockchain technology represents a sea change in how businesses will execute their transactions, it is imperative for managers to be cognisant of what adjustments or changes may be necessary to their current business processes and operational workflow designs to fully realise the value of blockchain. By cultivating an environment of creativity and acceptance to innovation, through communication methods and demonstration of management's commitment to innovation, will help mitigate departmental resistance and encourage employees to embrace blockchain technology with a positive mindset.

Human capital development. Managers of banks will need to develop, through training and up-skilling efforts, the capabilities of their personnel with respect to: blockchain technology, cyber-security, data governance, and the digital risk management associated with these operating environments. This in-house talent will reduce managers' reliance on third-party vendors and provide a greater degree of institutional integrity to the critical systems that underpin the bank's operations.

Additionally, collaboration provides banks with a number of benefits as a result of collaboration with other organizations. For instance, strategic partnerships with fintechs, technology service companies, and industry consortia will allow banks to leverage the capability and expertise of those companies, while at the same time helping them save money and expedite their projects.

7. Findings of the Study

Based on an extensive review of secondary academic literature, policy reports, and industry publications, this study identifies several key findings regarding the role of blockchain technology in enhancing security and transparency in banking transactions.

7.1 Enhancement of Transaction Security

The findings confirm that blockchain technology significantly strengthens transaction security within banking systems. The decentralised architecture of blockchain eliminates the single point of failure inherent in traditional centralised banking databases, thereby reducing vulnerability to cyberattacks, data manipulation, and unauthorised access. Cryptographic hashing, digital signatures, and consensus mechanisms ensure that transaction records are immutable and tamper-resistant once validated and recorded.

The study finds that distributed ledger technology (DLT) substantially reduces the risk of internal fraud and external cyber threats by preventing unauthorised alteration of transaction data. Consensus protocols such as Proof-of-Work (PoW), Proof-of-Stake (PoS), and permissioned consensus models used by financial institutions enhance validation accuracy and ensure that only legitimate transactions are processed. Consequently, blockchain contributes to improved data integrity, system resilience, and trust in banking transaction processes.

7.2 Improvement of Transparency and Auditability

A major finding of the study is that blockchain technology significantly enhances transparency across banking operations. Unlike traditional banking systems, where transaction records are fragmented across multiple intermediaries, blockchain provides a shared, real-time ledger accessible to authorised participants, including banks, auditors, and regulators.

The immutable and time-stamped nature of blockchain records creates a permanent audit trail that enables continuous auditing rather than periodic, sample-based audits. This increases accountability, simplifies reconciliation processes, and reduces operational costs associated with compliance and reporting. The findings suggest that blockchain-based transparency improves regulatory oversight and strengthens confidence among customers, regulators, and financial institutions.

7.3 Reduction of Fraud and Operational Risks

The study finds that blockchain technology plays a crucial role in fraud prevention and risk mitigation. The immutability of blockchain records allows anomalies and suspicious activities to be detected more easily, making fraudulent behaviour

traceable and identifiable. Smart contracts further reduce fraud risks by automating transaction execution based on predefined rules, thereby minimising human intervention and operational errors.

By reducing reliance on manual processing and intermediaries, blockchain lowers the likelihood of payment fraud, identity theft, and unauthorised transaction reversals. These characteristics make blockchain particularly effective in high-risk banking functions such as cross-border payments, trade finance, and interbank settlements.

7.4 Strengthening Data Integrity and Institutional Trust

The findings indicate that blockchain technology substantially improves data integrity across key banking functions, including payments, customer records, and compliance reporting. The distributed and immutable nature of blockchain ensures that transaction data cannot be altered, deleted, or manipulated without network consensus.

As a result, customer confidence in digital banking services increases, leading to stronger trust relationships between banks and their clients. Improved data integrity also enhances institutional reputation, reduces compliance risks, and supports long-term customer engagement in digital financial ecosystems.

7.5 Operational Efficiency and Banking Applications

The study finds that blockchain adoption improves operational efficiency by reducing settlement times, lowering transaction costs, and eliminating redundant reconciliation processes. Blockchain applications are particularly effective in cross-border payments, interbank settlements, trade finance, identity verification, and record management.

Real-time access to transaction data improves customer satisfaction and enables banks to provide faster, more reliable financial services. However, the findings also indicate that the full benefits of blockchain adoption depend on institutional readiness, technological infrastructure, and regulatory support.

7.6 Constraints to Effective Blockchain Adoption

Despite its advantages, the study finds that several challenges limit the widespread adoption of blockchain in banking. These include scalability constraints, high implementation costs, integration difficulties with legacy banking systems, cybersecurity risks related to smart contract design, and regulatory uncertainty across jurisdictions.

The findings suggest that permissioned or hybrid blockchain models are currently more suitable for banking applications, as they allow institutions to balance transparency with privacy and regulatory compliance.

Overall Finding

Overall, the study finds that blockchain technology has strong potential to transform banking transaction systems by simultaneously enhancing security, transparency, efficiency, and trust. However, successful implementation requires supportive regulatory frameworks, robust cybersecurity practices, institutional preparedness, and gradual integration with existing banking infrastructure.

8. Conclusion

This research analyzes how the implementation of blockchain technology may improve the security and transparency of banking transaction systems. This study shows that the unique features of blockchain (decentralization, cryptographic security, immutability, and distributed ledgers) will ultimately strengthen banking systems compared to traditional centralized models. The use of blockchain will provide tamper-proof record-keeping, instant verification of transactions, and automated execution of transactions, which together reduce the risk of fraudulent activity and improve data integrity while also increasing the confidence of all parties involved in financial transactions.

The study's findings also suggest that the adoption of blockchain technology can greatly improve the efficiency and transparency of banking operations (e.g., payments, settlements, trade finance, and audits). The ability to trace transactions provides greater visibility into and opportunities for regulatory compliance and quicker resolution of disputes. There are, however, a number of barriers to the widespread adoption of blockchain technology in banking, such as scalability, cybersecurity, lack of regulatory clarity, data privacy issues and the need to integrate with existing systems. These challenges will continue to prevent widespread adoption of blockchain technology in the banking sector until they are resolved.

Blockchain makes it possible to revolutionize modern banking through transforming across all levels; however, for this creation to be completed effectively it must have a balance of both technical innovation and governmental oversight within

an appropriate regulatory framework, as well as sufficient institutional preparedness. To create an appropriate climate for investing in both technical skills related to blockchain and digital infrastructure; therefore, it will be essential for financial policymakers and bank executives to work together to create an environment conducive to the development of safe and secure blockchain technologies, thereby providing greater accessibility and reliability in the development of these new systems. With an ongoing commitment to partnership and collaboration, it is likely that blockchain technology will provide a solid basis for a more trustworthy and secure banking system through its continued development in this digital era.

Funding

This research is supported by no specific grant or funding from any public, commercial, or not-for profit funding agencies. All activities associated with this research, including data collection, analysis, and manuscript preparation, were the independent work of the authors, completed within their scope of responsibility as academics.

Ethical Considerations

The authors assure that the research was conducted within the framework of accepted academic integrity and ethical practices. All data used in the study were acquired from secondary sources; such sources were publicly available and approved through ethical review. The authors did not collect data from human participants and therefore did not have to obtain informed consent for the study. Each source used in the manuscript has been properly cited to maintain compliance with intellectual property rights and to avoid any allegations of plagiarism.

Acknowledgments

The authors would like to express their appreciation to the Department of Commerce and Guru Ghasidas Vishwavidyalaya for their continuing support of academic and research excellence and for the facilitation of this research. They also wish to thank the academic community, including anonymous peer reviewers, who provided comments and constructive feedback, as well as the valuable insights of their colleagues, who contributed greatly to the development of this manuscript.

Conflict of Interest

The authors do not have any conflicts of interest with regard to the research, authorship, or publication of this manuscript.

References

1. Al Husseini, E. (2025). The potential of employing blockchain technologies in enhancing operational transparency of Iraqi banks. *International Journal of Finance & Banking Studies, 14*(4), 1–7. https://doi.org/10.20525/IJFBS.V14I4.4423
2. Arner, D. W., Barberis, J., & Buckley, R. P. (2017). FinTech, RegTech, and the reconceptualization of financial regulation. *Northwestern Journal of International Law & Business, 37*(3), 371–413. https://scholarlycommons.law.northwestern.edu/njilb/vol37/iss3/2
3. Bank for International Settlements. (2018). *Sound practices: Implications of fintech developments for banks and bank supervisors*. https://www.bis.org/bcbs/publ/d431.htm
4. Beck, T., Chen, T., Lin, C., & Song, F. M. (2016). Financial innovation: The bright and the dark sides. *Journal of Banking & Finance, 72*, 28–51. https://doi.org/10.1016/j.jbankfin.2016.06.012
5. Berryhill, J., Bourgery, T., & Hanson, A. (2018). *Blockchains unchained: Blockchain technology and its use in the public sector*. OECD Publishing. https://doi.org/10.1787/3c32c429-en
6. Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives, 29*(2), 213–238. https://doi.org/10.1257/jep.29.2.213
7. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification, and open issues. *Telematics and Informatics, 36*, 55–81. https://doi.org/10.1016/j.tele.2018.11.006
8. Chen, Y., Bellavitis, C., & Peltier-Rivest, D. (2021). Blockchain disruption and decentralized finance: The rise of decentralized business models. *Journal of Business Venturing Insights, 16*, e00247. https://doi.org/10.1016/j.jbvi.2021.e00247

9. Cong, L. W., & He, Z. (2019). Blockchain disruption and smart contracts. *Review of Financial Studies, 32*(5), 1754–1797. https://doi.org/10.1093/rfs/hhz007
10. Dewi, S., Firasati, A., Sitoayu, L., & Bennet, D. (2025). Risk management strategies in blockchain adoption within financial institutions: Analyzing challenges and opportunities. *APTISI Transactions on Management, 9*(1), 20–29. https://doi.org/10.33050/ATM.V9I1.2393
11. Gomber, P., Koch, J. A., & Siering, M. (2017). Digital finance and FinTech: Current research and future research directions. *Journal of Business Economics, 87*(5), 537–580. https://doi.org/10.1007/s11573-017-0852-x
12. International Monetary Fund. (2019). *FinTech: The experience so far*. IMF.
13. Johnston, M. P. (2014). Secondary data analysis: A method of which the time has come. *Qualitative and Quantitative Methods in Libraries, 3*(3), 619–626.
14. Kouhizadeh, M., Saberi, S., & Sarkis, J. (2021). Blockchain technology and the sustainable supply chain: Theoretically exploring adoption barriers. *International Journal of Production Economics, 231*, 107831. https://doi.org/10.1016/j.ijpe.2020.107831
15. Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. *Future Generation Computer Systems, 107*, 841–853. https://doi.org/10.1016/j.future.2017.08.020
16. Mendling, J., Weber, I., Van der Aalst, W., et al. (2018). Blockchains for business process management—Challenges and opportunities. *ACM Transactions on Management Information Systems, 9*(1), 1–16. https://doi.org/10.1145/3183367
17. Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org
18. Philippon, T. (2016). The fintech opportunity. *National Bureau of Economic Research Working Paper No. 22476*. https://doi.org/10.3386/w22476
19. Pilkington, M. (2016). Blockchain technology: Principles and applications. *Research Handbook on Digital Transformations*, Elsevier.
20. Sahay, R., Eriksson von Allmen, U., Lahreche, A., Khera, P., Ogawa, S., Bazarbash, M., & Beaton, K. (2020). *The promise of fintech: Financial inclusion in the post-COVID-19 era* (IMF Departmental Paper No. 20/09). IMF.
21. Saunders, M., Lewis, P., & Thornhill, A. (2023). *Research methods for business students* (9th ed.). Pearson Education.
22. Treleaven, P., Brown, R. G., & Yang, D. (2017). Blockchain technology in finance. *Computer, 50*(9), 14–17. https://doi.org/10.1109/MC.2017.3571047
23. Vives, X. (2019). Digital disruption in banking. *Annual Review of Financial Economics, 11*(1), 243–272. https://doi.org/10.1146/annurev-financial-100719-120854
24. Yermack, D. (2017). Corporate governance and blockchains. *Review of Finance, 21*(1), 7–31. https://doi.org/10.1093/rof/rfw074