

A Comparative Study of Traditional and Blockchain-Based Financial Transactions: Security, Transparency and Efficiency

P. S. Ghode¹, Anjali Rajkumar Talane², Sanskruthi Varahagiri Halvi³

Lecturer, Department of Information Technology¹

Diploma Students, Department of Information Technology²⁻³

Government Polytechnic Awasari (Khurd), Pune, Maharashtra, India

Abstract: *Traditional financial systems face several challenges, including transaction delays, high processing costs, dependence on intermediaries, reconciliation issues, limited transparency, fraud risks, data tampering, and complexity in cross-border transactions. Blockchain technology offers an alternative approach through a shared and distributed digital ledger. This paper compares traditional and blockchain-based financial transactions in terms of security, transparency, traceability, and efficiency. It also examines the potential role of smart contracts and discusses challenges such as scalability, privacy, regulatory uncertainty, and integration with existing systems. The study uses a qualitative comparative approach based on existing research literature. It concludes that blockchain may improve selected financial processes, depending on the application and implementation.*

Keywords: Blockchain Technology, Financial Transactions, Distributed Ledger Technology, Smart Contracts, Security, Transparency, Cross-Border Payments.

I. INTRODUCTION

The financial sector plays an important role in the modern economy by supporting banking, digital payments, money transfers, and other financial activities. Traditional financial systems often depend on banks and other intermediaries to process and verify transactions. However, these systems may face challenges such as transaction delays, high processing costs, reconciliation difficulties, limited transparency, and complexity in cross-border payments. Blockchain technology has emerged as a potential approach to address some of these challenges. It uses a distributed digital ledger to record transactions in a verifiable and tamper-resistant manner. Features such as transaction traceability and smart contracts may help improve transparency and automate selected financial processes. Previous studies have examined the opportunities and challenges of blockchain adoption in financial services [1], [2]. This paper compares traditional and blockchain-based financial transactions with a focus on security, transparency, data integrity, and efficiency. It also discusses the limitations of blockchain technology, including scalability, privacy, regulatory requirements, and integration with existing financial systems. The aim is to understand its potential benefits and challenges in financial applications.

II. PROBLEM STATEMENT

Traditional financial transactions often depend on multiple institutions for transaction verification, fund transfer, record maintenance, and settlement. When participating organizations maintain separate records, they may need additional reconciliation to confirm that transaction information is consistent. International transfers can involve further complications because of different banking arrangements, currencies, legal requirements, and compliance procedures. Security and transparency are also important concerns. Financial institutions must protect transaction records against unauthorized access, manipulation, and fraudulent activity. At the same time, institutions need appropriate access



controls to protect confidential customer information. Improving transparency without weakening privacy is therefore a significant operational requirement.

Blockchain technology offers a distributed approach to transaction recording and verification. However, its practical suitability depends on several factors, including transaction volume, network performance, privacy controls, implementation costs, interoperability, governance, and regulatory compliance.

The main problem addressed in this study is the need to understand how traditional and blockchain-based financial transactions differ in terms of security, transparency, data integrity, efficiency, and implementation requirements. A balanced comparison is necessary to identify where blockchain may provide practical value and where conventional financial systems may remain more suitable.

III. OBJECTIVES OF THE STUDY

- To study the basic characteristics and processes of traditional financial transactions.
- To explain the working principles and financial applications of blockchain technology.
- To compare traditional and blockchain-based financial transactions in terms of security, transparency, data integrity, efficiency, and reconciliation.
- To examine the potential role of smart contracts and distributed ledgers in selected financial processes.
- To identify the technical, operational, privacy, and regulatory challenges associated with blockchain adoption.
- To discuss the conditions under which blockchain may complement existing financial systems.

IV. RESEARCH METHODOLOGY

This study adopts a qualitative and comparative research approach based on secondary data. Information is collected from published research papers, academic journals, technical publications, and existing literature related to blockchain technology in financial services. The collected information is analyzed to compare traditional and blockchain-based financial transactions in terms of security, transparency, transaction efficiency, data integrity, reconciliation, and intermediary involvement. The study also examines potential applications and limitations of blockchain technology in financial transactions. No primary survey or experimental data is used in this research.

A. Research Design and Scope

The study follows a qualitative comparative research design. Its scope covers traditional financial transaction processes and blockchain-based approaches used or proposed for financial services. The comparison focuses on recordkeeping, transaction verification, security, transparency, data integrity, processing efficiency, reconciliation, and implementation requirements. It also considers smart contracts and cross-border financial transactions.

B. Data and Sources of Data

The research uses secondary information from published academic literature, review articles, technical publications, and research on financial applications of distributed ledger technology. The selected sources provide background on blockchain architecture, financial-sector applications, adoption challenges, and cross-border payment arrangements. The study does not claim to be a systematic review with an exhaustive database search or a statistically representative sample of all published studies.

C. Analytical Framework

The collected information is examined using selected qualitative dimensions:

Security: How transaction verification, access controls, and cryptographic mechanisms help protect financial records.

Transparency and traceability: How transaction histories can be reviewed by authorized participants.

Data integrity: How systems help detect unauthorized changes to recorded information.

Efficiency: How transaction processing, settlement, and coordination may be affected.



Reconciliation: Whether shared records may reduce the need to compare separate records maintained by different organizations.

Implementation requirements: How privacy, regulation, infrastructure, governance, and interoperability affect practical adoption.

D. Comparative Method

The two approaches are compared using a descriptive framework rather than a statistical or econometric model. Their characteristics are examined using existing literature and technical documentation. The comparison identifies potential advantages and limitations but does not claim to measure actual processing speed, cost savings, or security performance through a new experiment.

V. LITERATURE REVIEW

Existing research has examined blockchain technology from different perspectives, including financial applications, technical characteristics, cross-border transactions, and adoption challenges. The following studies provide the foundation for the present comparison.

A. Ali et al. (2020)

Ali et al. conducted a systematic literature review on blockchain technology in the financial services sector. Their study examined published research on blockchain-related financial benefits, challenges, and functionality. The authors reviewed an initial collection of 227 articles and selected 87 articles for their analysis. Their work provides a structured overview of how blockchain has been studied in financial services and identifies areas for future research [1].

Relevance to the present study: This research provides a foundation for examining both the opportunities and limitations of blockchain rather than focusing only on its potential benefits.

B. Pal et al. (2021)

Pal et al. presented a comprehensive review of blockchain technology in financial services using a systematic literature review and bibliometric analysis. Their work organized existing research to understand the development of blockchain-related financial applications and the challenges affecting adoption [2].

Relevance to the present study: Their review supports the need to examine blockchain as part of the wider financial-services environment, including the organizational and technical conditions required for implementation.

C. Zhang (2020)

Zhang examined blockchain-based cross-border financial transactions and considered the legal and regulatory arrangements relevant to their development. The study discussed the importance of a suitable regulatory framework for international financial transactions involving blockchain technology [3].

Relevance to the present study: This work highlights that cross-border transaction improvements depend not only on technology but also on legal coordination and compliance across jurisdictions.

D. Rahman et al. (2025)

Rahman et al. studied factors influencing blockchain adoption in the banking industry through a systematic review and bibliographic network mapping. Their research identified three broad themes: transparency-driven security, collaborative interoperability, and organizational infrastructure. The study emphasized that adoption depends on more than technical capabilities alone [4].

Relevance to the present study: These themes support the inclusion of security, interoperability, governance, and implementation requirements in the comparative framework.

E. Technical and Regulatory Perspectives

The National Institute of Standards and Technology (NIST) describes blockchain as a distributed ledger in which cryptographically linked blocks and network validation mechanisms help make recorded information tamper-evident and tamper-resistant [5]. This technical perspective is useful for understanding data integrity and transaction verification.



The Bank for International Settlements has examined the legal and regulatory considerations associated with distributed-ledger-based cross-border payments. Its research identifies possible applications while emphasizing the importance of legal responsibilities, compliance, and coordination among participating entities [6].

F. Research Gap

The reviewed literature provides important insights into blockchain applications, adoption factors, technical characteristics, and regulatory challenges. However, the present study takes a focused comparative approach by organizing these issues around traditional and blockchain-based financial transaction processes.

Its contribution is a consolidated qualitative comparison across security, transparency, data integrity, efficiency, reconciliation, and implementation requirements. The study also distinguishes potential technical benefits from outcomes that depend on the specific network, application, and operating environment. It does not claim that earlier research has ignored comparative analysis entirely; rather, it uses a focused framework to present these dimensions together.

VI. TRADITIONAL FINANCIAL TRANSACTIONS AND THEIR CHALLENGES

Traditional financial transactions are generally processed through banks, payment service providers, card networks, clearing systems, and other authorized institutions. These organizations perform functions such as customer verification, transaction authorization, record maintenance, payment processing, and settlement. The exact process varies according to the payment method and the financial institutions involved.

A. Centralized Recordkeeping

In many traditional arrangements, individual institutions maintain their own transaction databases and accounting records. Each institution is responsible for the accuracy, security, and availability of its records. When a transaction involves multiple organizations, information may need to be exchanged and compared to ensure that the records agree.

B. Transaction Verification and Settlement

Transactions may require several stages, including identity verification, authorization, clearing, and settlement. These stages are important for managing financial risk and ensuring that transactions comply with applicable rules. However, the involvement of multiple institutions and operating schedules can affect the time required for final settlement.

C. Reconciliation and Operational Costs

Financial institutions periodically compare transaction records to identify discrepancies and confirm that balances are consistent. Differences between records may require investigation and correction. These activities consume operational resources. Transaction costs may also include processing charges, service fees, currency conversion charges, and intermediary fees, depending on the transaction.

D. Transparency and Traceability

Transaction information is generally accessible according to institutional policies, customer permissions, and legal requirements. Customers can obtain information through statements or transaction interfaces, while authorized institutions can access records relevant to their responsibilities. However, different organizations may maintain separate systems, which can complicate end-to-end tracking.

E. Security and Cross-Border Challenges

Traditional systems use authentication, access controls, monitoring, encryption, auditing, and regulatory procedures to protect financial activities. Nevertheless, risks such as stolen credentials, phishing, unauthorized access, and fraudulent instructions can still occur.

Cross-border transactions may require coordination among multiple institutions and compliance with different jurisdictions. Currency conversion, payment-network arrangements, identity checks, and regulatory obligations may add complexity. These challenges provide a reason to investigate alternative methods of record sharing and transaction coordination, but they do not mean that every traditional transaction is slow, costly, or insecure.



VII. BLOCKCHAIN-BASED FINANCIAL TRANSACTIONS

Blockchain is a type of distributed ledger technology that records transactions in a shared digital record maintained by participating network nodes. Transactions are validated according to the rules of the particular network. Validated records are grouped into blocks, and cryptographic links connect the blocks to earlier records. This structure helps make unauthorized changes detectable [5].

A. Distributed Ledger and Transaction Validation

Unlike a system in which a single institution maintains the only authoritative transaction database, a blockchain network can distribute copies of the ledger across multiple participating nodes. When a transaction is submitted, the network checks it according to its validation rules. The method used to agree on valid transactions depends on the network's consensus mechanism and governance model.

Public blockchains may permit broad participation, while permissioned blockchains restrict participation or particular activities to approved entities. This distinction is important in financial services because institutions often need controlled access, confidentiality, accountability, and compliance with regulatory requirements.

B. Cryptography and Data Integrity

Blockchain systems use cryptographic techniques to protect transaction information and link records. A cryptographic hash produces a fixed-length representation of data; changing the underlying data changes the resulting hash. Because blocks are linked, altering a previously recorded block can disrupt the links to subsequent blocks and make the change detectable.

However, tamper resistance is not the same as complete security. Blockchain cannot independently guarantee that information entered into the system was accurate. Compromised accounts, stolen private keys, vulnerable software, and poorly designed applications can still create risks.

C. Smart Contracts

Smart contracts are programs deployed on a blockchain network that execute predefined operations when specified conditions are met. In financial applications, they may support payment release, settlement instructions, asset transfers, and other rule-based processes.

For example, a smart contract could be designed to release a digital asset when the required payment condition is confirmed. Such automation may reduce some manual steps, but its reliability depends on correct programming, valid input data, suitable access controls, and appropriate legal arrangements.

D. Applications in Financial Services

Digital payments and transfers: Blockchain-based systems may support the transfer of digital assets between participating users or institutions. The actual payment experience depends on network design, asset type, conversion arrangements, and compliance requirements.

Cross-border payments: Distributed-ledger arrangements may help coordinate transaction records among participating organizations. However, they do not automatically eliminate foreign-exchange requirements, identity checks, legal obligations, or the need to connect with local payment systems [3], [6].

Settlement and reconciliation: A shared ledger can provide participating institutions with a common transaction record. If the institutions rely on that record for the relevant process, some duplicated record comparison may be reduced.

Trade finance: Blockchain may be used to share transaction records and coordinate selected processes among importers, exporters, banks, and other participants. Its usefulness depends on reliable documentation, participant cooperation, and integration with existing systems.

Digital asset management: Distributed ledgers can record ownership transfers and support the management of certain digital assets. Appropriate custody, identity, legal, and operational arrangements remain necessary.

E. Potential Operational Benefits

The main potential benefits of blockchain in financial transactions include shared recordkeeping, transaction traceability, tamper-evident records, and automation of selected predefined processes. These features may improve



coordination when several organizations need to rely on consistent transaction information. The benefits are conditional, however, and must be evaluated for the specific financial application.

VIII. COMPARATIVE ANALYSIS

Traditional and blockchain-based financial transactions differ in their recordkeeping arrangements, validation processes, access models, and coordination requirements. Table I summarizes their general characteristics. Actual performance depends on the specific traditional payment system or blockchain network being considered.

TABLE I: Comparison of Traditional and Blockchain-Based Financial Transactions

Parameter	Traditional Financial System	Blockchain-Based Approach
Recordkeeping	Records are maintained by individual institutions or connected systems.	Participating nodes maintain a shared ledger according to network rules.
Transaction verification	Performed by banks, payment networks, or designated intermediaries.	Performed through the network's validation and consensus rules.
Transparency	Visibility depends on institutional access, permissions, and policies.	Records may be visible to authorized participants or publicly, depending on the network.
Data integrity	Supported by access controls, auditing, backups, and institutional security.	Cryptographic linking can help make unauthorized changes detectable.
Reconciliation	Separate records may need to be compared across organizations.	Shared records may reduce some reconciliation between participating organizations.
Transaction costs	May include processing, service, currency conversion, and intermediary fees.	May reduce selected costs but can introduce network, integration, and governance costs.
Cross-border transfers	May involve multiple institutions, payment networks, and compliance processes.	May improve coordination in some arrangements, but legal and currency requirements remain.
Automation	Uses established banking software and payment rules.	Smart contracts can automate selected predefined operations.
Privacy	Managed through institutional policies, permissions, and data-protection controls.	Depends on network type, data design, permissions, and privacy mechanisms.
Implementation	Uses established infrastructure and operating procedures.	May require new infrastructure, integration, expertise, and governance arrangements.
Operational responsibility	Roles and responsibilities are assigned to institutions and service providers.	Responsibilities must be defined across network operators, participants, developers, and service providers.
Modification and correction	Records can be corrected through authorized institutional procedures and audit trails.	Recorded history may be difficult to alter; corrections may require additional transactions or defined governance procedures.

A. Security and Data Integrity

Traditional financial systems rely on institutional security controls, monitoring, authentication, and established procedures. Blockchain adds a different approach to maintaining a shared transaction history, with cryptographic linking and network validation helping to detect unauthorized modification. Neither approach removes all security risks. The comparison must therefore consider the full system, including users, applications, infrastructure, and governance.



B. Transparency and Privacy

A shared ledger may make transaction histories easier to verify among participating institutions. However, transparency must be balanced against confidentiality. Public visibility may be inappropriate for sensitive financial information, while permissioned networks require clear rules governing who can access records. Traditional systems can also provide detailed audit trails and controlled access. The suitability of each approach depends on the information that must be shared and the parties authorized to view it.

C. Efficiency and Reconciliation

Blockchain may reduce the need to compare separate transaction records when participants rely on a common ledger. Smart contracts may also automate specific rule-based operations. Nevertheless, transaction throughput, confirmation time, integration requirements, and network fees vary between blockchain systems. A traditional payment system may remain more efficient for some high-volume or well-established use cases.

D. Intermediaries and Governance

Blockchain may redistribute some verification or recordkeeping functions among network participants. It does not necessarily remove intermediaries. Banks, custodians, payment providers, exchanges, identity-verification services, and regulatory authorities may still be required. The important question is whether the new arrangement improves coordination and accountability for the particular transaction.

Overall, blockchain offers a different model for sharing and validating transaction records. Its practical value depends on whether these characteristics solve a specific operational problem more effectively than the existing system.

IX. RESULTS AND DISCUSSION

The qualitative comparison and reviewed literature indicate that blockchain may provide useful capabilities for selected financial transaction processes. The main observations are discussed below.

A. Shared Recordkeeping Can Support Coordination

When multiple organizations maintain separate transaction records, they may need to compare those records to confirm that information is consistent. A shared ledger can provide a common record for participating organizations, potentially reducing some duplicated reconciliation activities. This benefit depends on whether participants agree to use the shared record and whether it contains the information needed for their processes.

B. Tamper-Evident Records Can Support Auditing

Cryptographic linking and network validation can make unauthorized modifications to recorded blockchain data detectable. This characteristic may help support auditing and traceability. However, it does not prove that the original transaction information was correct, nor does it prevent all forms of fraud. Accurate data entry, identity verification, secure applications, and proper governance remain essential.

C. Automation Can Reduce Selected Manual Steps

Smart contracts can execute predefined rules, which may help automate selected payment or settlement activities. Their usefulness is greatest when the conditions are clearly defined and can be verified reliably. Complex financial arrangements may still require human review, legal interpretation, exception handling, and external information.

D. Cross-Border Applications Require Wider Coordination

Blockchain-based arrangements may help participating institutions share transaction information and coordinate selected stages of a cross-border transfer. However, the transaction still operates within a broader environment involving currency conversion, customer identification, sanctions screening, local regulations, and connections to existing payment infrastructure. Technical coordination alone cannot resolve every legal or operational obstacle [6].

E. Blockchain Is Not a Universal Replacement

The findings do not establish that blockchain is always faster, cheaper, or more secure than traditional financial systems. Its performance depends on network architecture, transaction volume, governance, and implementation quality. Traditional systems may be preferable where established infrastructure, predictable performance, clear institutional accountability, and existing regulatory arrangements already meet operational needs.



The overall finding is that blockchain should be assessed against a defined financial problem and measurable requirements. Decisions about adoption should consider the complete transaction lifecycle rather than the ledger technology alone.

X. CHALLENGES AND LIMITATIONS

Despite its potential, blockchain technology faces several challenges that may limit its suitability for financial services.

A. Scalability and Performance

Some blockchain networks may face limits on transaction throughput or experience longer confirmation times as demand increases. Performance depends on the consensus mechanism, network capacity, and transaction design. A system suitable for a limited network may not be appropriate for a high-volume payment environment without further development.

B. Privacy and Confidentiality

Financial transactions can contain sensitive information about individuals and organizations. Sharing transaction records across a network creates a need for careful privacy design. Permissioned access, data minimization, and appropriate cryptographic or privacy-preserving techniques may help, but they require proper implementation and evaluation.

C. Regulatory and Legal Uncertainty

Financial activities are subject to laws and regulatory requirements that may differ across jurisdictions. Blockchain arrangements can distribute technical responsibilities among multiple participants, raising questions about accountability, dispute resolution, data protection, and compliance. Cross-border arrangements require particular attention to these issues [3], [6].

D. Integration and Interoperability

Financial institutions already operate established payment platforms, databases, identity systems, and accounting processes. Integrating blockchain with these systems may require investment, technical expertise, and changes to existing workflows. Different blockchain networks may also lack seamless interoperability, limiting the benefits of a shared-ledger approach.

E. Security Risks Beyond the Ledger

Blockchain's tamper-resistant structure does not guarantee that every component of a financial application is secure. Stolen private keys, compromised user accounts, vulnerable smart contracts, malicious software, and inaccurate external data can cause financial losses. Effective security requires controls across the entire application and operational environment.

F. Cost and Organizational Readiness

Implementation may require infrastructure, skilled personnel, testing, maintenance, governance arrangements, and staff training. These costs can outweigh potential benefits if the use case is poorly selected. Organizations should evaluate total lifecycle costs rather than assuming that removing some intermediaries will automatically make a transaction cheaper.

G. Limitations of the Present Study

This study is based on secondary literature and qualitative comparison. It does not include a primary survey, experimental implementation, transaction-level dataset, or statistical performance evaluation. Consequently, it cannot provide measured estimates of transaction speed, cost savings, or security improvements. The findings should be interpreted as a comparative assessment of potential capabilities and limitations rather than empirical proof of performance superiority.



XI. FUTURE SCOPE

Future research can examine blockchain applications in cross-border payments, interbank settlement, trade finance, digital asset transfers, and other financial processes where multiple organizations need to coordinate transaction records.

Quantitative studies could compare processing time, transaction fees, settlement time, failure rates, and reconciliation effort under clearly defined conditions. Such studies should specify the traditional payment method and the blockchain network being compared so that results are meaningful and reproducible.

Further research may also investigate privacy-preserving techniques, interoperability between blockchain networks, integration with existing banking infrastructure, and governance models for permissioned networks. Smart contracts could be evaluated for selected financial processes, with particular attention to testing, error handling, security, and regulatory compliance.

Case studies involving financial institutions and payment service providers could help identify the operational conditions under which blockchain provides measurable benefits. Research focused on user protection, accountability, and dispute resolution could further clarify how distributed-ledger arrangements should be designed for regulated financial services.

XII. CONCLUSION

This study has compared traditional and blockchain-based financial transactions in terms of security, transparency, data integrity, efficiency, reconciliation, and implementation requirements. The analysis shows that blockchain offers a distributed approach to recording and validating transactions, with potential benefits in shared recordkeeping, traceability, and automation of selected financial processes.

A shared ledger may reduce some reconciliation activities between participating organizations, while cryptographic mechanisms can help make unauthorized changes to recorded information detectable. Smart contracts may also automate predefined operations when appropriate conditions are satisfied. However, these capabilities do not automatically guarantee faster transactions, lower costs, complete privacy, or the elimination of fraud.

Blockchain adoption remains subject to challenges involving scalability, confidentiality, interoperability, regulatory compliance, integration, security, and organizational readiness. Traditional financial systems continue to provide established infrastructure, institutional responsibilities, and operating procedures. Their suitability should therefore be evaluated alongside the potential capabilities of blockchain.

The study concludes that blockchain should be considered a potential complementary approach for financial processes where shared verification, traceability, and coordinated recordkeeping provide clear value. Its adoption should be guided by the specific requirements of the financial application, careful assessment of risks and costs, and compliance with relevant legal and regulatory obligations.

REFERENCES

1. O. Ali, M. Ally, P. Clutterbuck, and Y. Dwivedi, "The State of Play of Blockchain Technology in the Financial Services Sector: A Systematic Literature Review," *International Journal of Information Management*, vol. 54, article 102199, 2020. doi: 10.1016/j.ijinfomgt.2020.102199.
A. Pal, C. K. Tiwari, and A. Behl, "Blockchain Technology in Financial Services: A Comprehensive Review of the Literature," *Journal of Global Operations and Strategic Sourcing*, vol. 14, no. 1, pp. 61–80, 2021. doi: 10.1108/JGOSS-07-2020-0039.
2. Y. Zhang, "Developing Cross-Border Blockchain Financial Transactions under the Belt and Road Initiative," *The Chinese Journal of Comparative Law*, vol. 8, no. 1, pp. 143–176, 2020. doi: 10.1093/cjcl/cxaa010.
3. S. M. M. Rahman, A. N. M. Saif, S. Kabir, M. F. Bari, M. M. Alom, M. J. Rayhan, F. Zan, M. Chu, and A. Talukder, "Blockchain in the Banking Industry: Unravelling Thematic Drivers and Proposing a Technological



Framework through Systematic Review with Bibliographic Network Mapping,” *IET Blockchain*, vol. 5, no. 1, article e12093, 2025. doi: 10.1049/blc2.12093.

4. D. Yaga, P. Mell, N. Roby, and K. Scarfone, *Blockchain Technology Overview*. NIST Interagency/Internal Report 8202, National Institute of Standards and Technology, 2018. doi: 10.6028/NIST.IR.8202.
5. L. Anker-Sørensen, M. L. Passador, and A. Wehrli, *DLT-Based Enhancement of Cross-Border Payment Efficiency: A Legal and Regulatory Perspective*. BIS Working Papers, no. 1015, Bank for International Settlements, 2022

