Jurnal Penelitian Sains Teknologi

Utilization of Blockchain-Based Smart Contracts in Banking: A Systematic Review of Technical, Regulatory, and Systemic Risk Dimensions

Fajar Gemilang Pradana[1]✉, Taqiya Dipsatara[2]

[1]Faculty of Computer Science, Universitas Amikom Yogyakarta, Indonesia
[2]Faculty of Economics, Social Sciences, and Humanities, Universitas Muhammadiyah PKU Surakarta, Indonesia

doi: 10.23917/saintek.v2i2.16341
Received: January 15th, 2026 | Revised: February 25th, 2026 | Accepted: February 28th, 2026
Available Online: March 6th, 2026 | Published Regularly: September, 2026

Abstract

The advancement of blockchain technology has created significant opportunities for transforming the financial sector, particularly banking. One of the most transformative applications of this technology is the smart contract—self-executing digital agreements that automatically enforce predefined conditions without the need for intermediaries. This study presents a systematic literature review of 10 academic publications published between 2020 and 2025 to evaluate the utilization of smart contracts in the banking sector. The analysis focuses on three main dimensions: technical implementation, regulatory compliance, and systemic risk implications. The findings indicate that smart contracts have been implemented in automated lending systems, decentralized identity verification (KYC), asset tokenization, real-time auditing, and blockchain-based payment infrastructures. Despite these advantages, adoption remains constrained by security vulnerabilities in contract code, scalability limitations, interoperability challenges, and regulatory uncertainty across jurisdictions. This study also proposes a conceptual experimental framework for evaluating smart contract performance, security robustness, and compliance readiness within banking environments. The results contribute to a more integrated understanding of how smart contracts can be adopted safely and sustainably in highly regulated financial ecosystems.

Keywords: blockchain, smart contracts, banking systems, financial technology, systemic risk.

✉**Corresponding Author:**
Fajar Gemilang Pradana, Faculty of Computer Science, Universitas Amikom Yogyakarta, Indonesia
Email: fajarpradana@students.amikom.ac.id

Introduction

The banking sector has become one of the fields most significantly impacted by technological disruption amid the rapid pace of the digital revolution. Financial institutions no longer rely solely on conventional systems but are required to adapt to a new ecosystem that is faster, more transparent, and more secure [1]. In this context, blockchain technology offers a novel approach to how transactions and contracts are executed [2].

One of the most prominent innovations within the blockchain ecosystem is the smart contract. This technology refers to a digital protocol capable of automatically executing agreements once predefined conditions are met. Unlike traditional contracts that require third-party verification, smart contracts operate autonomously on blockchain networks, based on the fundamental principle of decentralized trust [3] [4].

The implementation of smart contracts in the banking sector is not merely a symbol of innovation, but also a response to longstanding challenges that have not been optimally resolved. Administrative delays, reliance on physical documentation, and risks of data manipulation all highlight the need for more efficient and trustworthy systems [5].

Currently, various banks worldwide have begun exploring the potential of smart contracts to automate lending processes, streamline Know Your Customer (KYC) procedures, and support more efficient cross-border transactions [6]. In several case studies, smart contracts have also been utilized for asset tokenization, real-time audit reporting, and automated payment systems free from manual intervention [7]

However, like other emerging technologies, the implementation of smart contracts presents its own challenges. A major concern lies in code security, where vulnerabilities such as reentrancy attacks, integer overflow, and flawed contract logic may result in substantial financial losses [8] [9]. In addition, regulatory uncertainty and differences in legal frameworks across jurisdictions hinder widespread adoption [10].

Furthermore, integrating smart contracts with complementary technologies such as Artificial Intelligence (AI) and the Internet of Things (IoT) remains challenging. A comprehensive approach is required to ensure that these systems operate harmoniously within the complex and highly regulated banking ecosystem [11].

Although several major banks have conducted pilot projects and even implemented smart contracts in limited operational contexts, there remains a lack of academic studies that systematically evaluate the effectiveness, risks, and readiness of this technology for comprehensive adoption in the banking sector [12] [13]. Most existing publications tend to focus on technical aspects or isolated case studies, without providing a holistic overview of trends, challenges, and future development directions.

Several previous Systematic Literature Review (SLR) studies have examined blockchain and smart contract applications in the broader fintech context, covering sectors such as digital payments, supply chain finance, crowdfunding, and decentralized finance (DeFi). However, these studies generally adopt an aggregated perspective and do not specifically analyze the distinctive characteristics of the banking industry, which involves regulatory complexity, risk governance frameworks, and legacy infrastructures that differ from other fintech sectors. Moreover, most prior SLRs primarily emphasize technical aspects or operational efficiency, without integrating a multidimensional analysis encompassing technical implementation, regulatory compliance (e.g., data protection and prudential banking principles), and systemic risk implications in the event of large-scale smart contract failure. This gap highlights the need for a systematic review that specifically maps the utilization of smart contracts in the banking context using a more comprehensive and integrated approach.

Based on these considerations, this study aims to conduct a systematic review of smart contract utilization in the banking sector. Through the screening and analysis of ten academic publications published between 2020 and 2025, this research seeks to summarize how smart contracts have been, are being, and may potentially be applied in various financial scenarios.

Rather than merely listing potential benefits, this study critically examines the primary barriers faced by financial institutions in implementing smart contracts. Regulatory aspects, technical challenges, and infrastructure readiness constitute key focal points of the discussion, while also highlighting strategic opportunities available to stakeholders.

In conducting this review, the authors adopted a systematic approach following the principles of the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA). The process included comprehensive literature searches across academic databases, screening based on predefined inclusion and exclusion criteria, and thematic analysis of the selected studies.

Through this approach, the findings are expected to provide meaningful contributions for both academics interested in financial technology research and banking practitioners considering broader smart contract adoption. Additionally, the results may serve as an initial reference for regulators in formulating adaptive policies that remain aligned with consumer protection principles.

It is important to recognize that smart contracts are not a universal solution capable of resolving all banking challenges simultaneously. However, with proper understanding and careful implementation, this technology has the potential to become a new foundation for building a more transparent, inclusive, and efficient financial system.

More than merely a technological trend, smart contracts represent a deeper spirit of digital transformation where efficiency meets trust, and technology functions not as a replacement for humans, but as a facilitator of fairness and precision within the financial sector.

Through this research, the authors seek to open broader discussions regarding the future direction of smart contract technology within the banking ecosystem. Will smart contracts become the new operational norm in banking, or will they remain technological experiments that struggle to integrate with legal and social realities?

By considering multiple dimensions, this article comprehensively examines how smart contracts have shaped a new landscape in banking and explores the possibilities that lie ahead. This review is not only retrospective but also serves as a reflective guide for future development.

Method

This study adopts a Systematic Literature Review (SLR) approach to collect, evaluate, and synthesize relevant academic literature concerning the utilization of smart contracts in the banking sector. This approach enables a structured and comprehensive analysis of implementation trends, existing challenges, and proposed solutions identified in previous studies.

a. Research Questions

As the foundation of this systematic review, the study is designed to address the following three primary research questions:

- **RQ1:** What forms of smart contract implementation exist within banking systems?

- **RQ2:** What security challenges most frequently arise in smart contract implementation?
- **RQ3:** How do regulatory frameworks support or hinder the adoption of smart contracts in the banking sector?

These research questions guide the literature identification process and content analysis, while facilitating a more comprehensive understanding of the dynamics of smart contract implementation within the financial industry.

b. Literature Search and Selection Strategy

The literature search was conducted across several reputable academic databases, including IEEE Xplore, MDPI, Springer, Emerald Insight, RESTI, and arXiv. The keywords used in the search process included: *"smart contract," "blockchain banking,"* and *"systematic review."* These keywords were applied in combination to ensure broad yet relevant coverage of the topic.

The retrieved literature was subsequently screened based on the following inclusion criteria:

a. Published between 2020 and 2025.
b. Written in English or Indonesian.
c. Specifically discussing the implementation of smart contracts in banking and finance.
d. Classified as case studies, systematic reviews, or technological framework development studies.

The initial screening process was conducted through title, abstract, and keyword evaluation to ensure alignment with the research focus. Publications that were duplicated or failed to meet the inclusion criteria were excluded from further analysis.

c. Study Selection Process

The study selection process followed the PRISMA 2020 guidelines to ensure transparency and reproducibility. The study selection flow diagram is presented in the following figure.

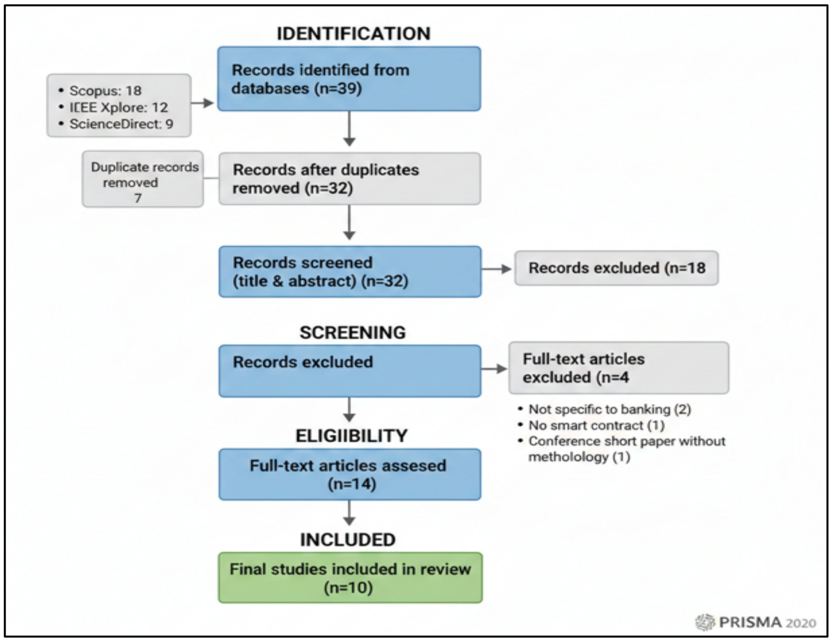
IDENTIFICATION
Records identified from databases (n=39)
• Scopus: 18
• IEEE Xplore: 12
• ScienceDirect: 9
Duplicate records removed 7
Records after duplicates removed (n=32)
Records screened (title & abstract) (n=32)
Records excluded (n=18
SCREENING
Records excluded
Full-text articles excluded (n=4
• Not specific to banking (2)
• No smart contract (1)
• Conference short paper without metholology (1)
ELIGIIBILITY
Full-text articles assesed (n=14)
INCLUDED
Final studies included in review (n=10)
PRISMA 2020

Figure 1. Prisma Flow Diagram

Result and Discussion

a. Quality Assessment

To ensure the quality and validity of the analyzed literature, a Quality Assessment (QA) process was conducted for all articles that passed the selection stage. The assessment was carried out using five primary criteria: (1) clarity of research objectives, (2) clarity of methodology, (3) relevance to the banking context, (4) validity of evaluation or empirical evidence, and (5) scientific contribution provided.

Table 1. Quality Assessment

No	Author (Year)	QA1	QA2	QA3	QA4	QA5	Total	Category
1	Ashtiani (2024)	2	2	2	1	2	9	High
2	Yatsenko (2022)	2	1	2	1	1	7	Medium
3	Rossi (2021)	2	1	2	1	2	8	High
4	Virani (2022)	2	2	1	2	2	9	High
5	Susanto (2022)	1	1	2	1	1	6	Medium
6	Zhang (2022)	2	1	2	1	1	7	Medium
7	Ibekwe (2024)	2	2	1	2	2	9	High
8	Nakamura (2020)	2	1	2	1	2	8	High
9	Robusti (2025)	2	1	1	1	1	6	Medium
10	Park (2023)	2	1	2	1	1	7	Medium

Each criterion was evaluated using a three-point scale (0–2), where a score of 2 indicates strong fulfillment of the criterion, 1 indicates partial fulfillment, and 0 indicates that the criterion was not met. The maximum possible score for each article was 10.

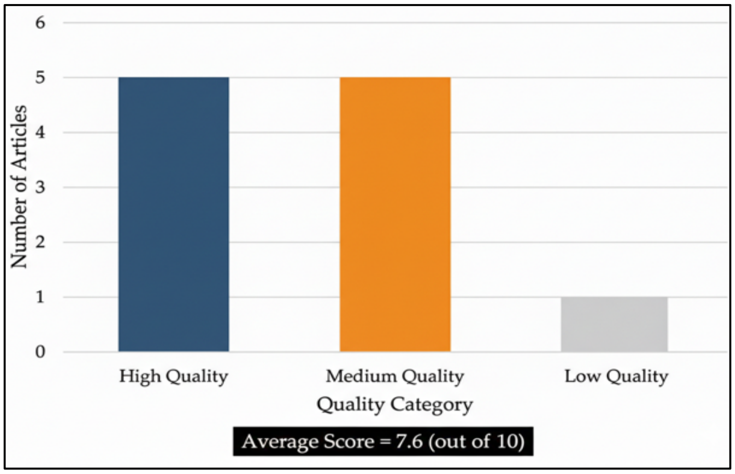

Figure 2. Distribution of Quality Assessment Results

Based on the evaluation results, the articles were categorized into three quality levels: High (8–10), Medium (5–7), and Low (0–4). Articles classified as Low quality were excluded from the final analysis. Of the 10 analyzed articles, categorized 50% as High Quality and 50% as Medium Quality, with an overall average score of 7.6. These results indicate that the selected literature demonstrates an adequate level of methodological validity

b. Smart Contract Implementation in Banking

Smart contracts have demonstrated various forms of implementation within banking and financial services. Several applications are summarized in the following table.

Table 2. Smart Contract Implementation

Application	Brief Description	References
Loan Automation	Loan processing, disbursement, and repayment are executed automatically through smart contract mechanisms	Yatsenko et al. (2022); Ashtiani et al. (2024)
Decentralized KYC	Identity verification is conducted across institutions without exchanging sensitive customer data	Susanto et al. (2022)
Automated Recurring Payments	Payment scheduling and billing are automatically executed without manual intervention	Ashtiani et al. (2024); Ambekar et al. (2024)
Financial Asset Tokenization	Assets such as bonds are digitally represented and can be traded more efficiently	Kovalenko et al. (2024); Robusti (2025)
Real-Time Automated Auditing	Immutable transaction recording supports real-time audit processes	Rossi (2021); Dominguez et al. (2024)
Blockchain-Based Crowdfunding	Funds are released only when predefined contractual conditions are fulfilled	Aprialim (2020); Weerapperuma (2025)

These implementations not only improve internal banking efficiency but also enhance service transparency and reliability for customers.

c. Supporting Technological Components

For smart contracts to function optimally within banking systems, several supporting infrastructures and technological components are required:

1. Blockchain Layer: Responsible for recording transactions and ensuring data integrity through decentralized mechanisms [14].
2. Contract Logic: The programmed code representing business logic and transactional rules executed automatically by the system [15].
3. Oracles: Bridging components between the blockchain and external data sources, enabling smart contracts to make decisions based on real-world information [16].
4. Security Analysis Tools: Tools such as Mythril, Slither, and Oyente are employed to detect potential vulnerabilities within smart contract code prior to deployment [3] [17].

d. Security Analysis

Despite offering significant efficiency gains, smart contracts present substantial security risks:

1. Reentrancy Attacks: Attacks that allow a contract to be repeatedly invoked before a previous transaction is completed, potentially leading to transaction duplication or unauthorized fund withdrawals [6].
2. Integer Overflow/Underflow: Arithmetic errors caused by data type limitations that may go undetected by the system.
3. Complex Contract Design: The more complex the contract structure, the higher the likelihood of hidden bugs and logical vulnerabilities.

To mitigate these risks, security testing is conducted using analysis tools such as Mythril, Slither, and Oyente to ensure that contracts are free from critical vulnerabilities before being deployed on the main network.

e. Regulatory Role

Regulatory aspects play a vital role in the adoption of smart contracts. The analyzed studies indicate that:

1. Smart contracts have not yet been legally recognized in many jurisdictions.
2. Data privacy regulations such as the General Data Protection Regulation (GDPR) remain reference frameworks, although their implementation is not globally uniform.
3. Several countries have begun establishing regulatory sandboxes to provide controlled environments for testing blockchain-based financial technologies.
4. In the absence of adaptive and supportive legal frameworks, smart contract implementation remains vulnerable to legal uncertainty and institutional trust barriers [18].

f. Experimental Design for Smart Contract Evaluation

Although this study is literature-based, the authors propose a conceptual experimental design to evaluate the performance, security, and compliance of smart contracts within banking systems. This design is not intended as an empirical implementation within the current study, but rather as an evaluative framework that may be adopted in future research to validate the synthesized findings.

The proposed experiment focuses on three primary testing dimensions: (1) system performance evaluation, (2) contract security validation, and (3) operational compliance and auditability. These dimensions reflect the characteristics of banking systems, which require high throughput, low fault tolerance, and strict regulatory compliance.

The prototype architecture is designed under two implementation scenarios: a public blockchain and a permissioned blockchain, enabling comparative analysis of their respective characteristics within the banking context.

Table 3. Prototype Architecture

Component	Specification	Function
Blockchain Platform	Ethereum (public), Hyperledger Fabric (permissioned)	Infrastructure for smart contract execution
Programming Language	Solidity (Ethereum), Chaincode in Go/Java (Hyperledger)	Development of contract logic
Smart Contract Modules	Loan origination, installment payment automation, penalty enforcement	Automation of credit processes
Audit Trail Module	Event logging & immutable ledger	Transaction traceability and regulatory compliance
API Layer	RESTful API	Integration with core banking systems
Off-chain Database	SQL/NoSQL database	Storage of sensitive non-transactional data
Node Configuration	4–8 validator nodes	Simulation of a consortium banking environment

This architecture adopts a hybrid approach, in which primary transaction data are recorded on-chain to ensure integrity and non-repudiation, while sensitive customer data are stored off-chain to maintain compliance with data protection regulations.

The proposed experimental design is conceptual in nature and intended as a recommendation for future research development. Empirical implementation and real-world testing within banking environments would require institutional collaboration and more complex regulatory considerations.

Performance testing is designed using the following parameters:

1. Throughput (Transactions Per Second / TPS)

Measures the number of loan or installment payment transactions that can be processed per second.

2. Latency (ms)

Measures the average transaction confirmation time from initiation to finality.

3. Gas Consumption / Resource Utilization

On Ethereum, gas consumption for each smart contract function is analyzed. On Hyperledger Fabric, CPU and memory utilization of validator nodes are evaluated.

4. Scalability Test

Simulation of increasing transaction loads (100–10,000 concurrent transactions) to evaluate performance degradation under stress conditions.

g. Testing Environment

1. Ganache & Truffle: Used to simulate a local Ethereum network environment.
2. MetaMask: User interface for interacting with deployed smart contracts.
3. Mythril & Slither: Security analysis tools used to detect potential vulnerabilities in smart contract code.

Table 4. Evaluation Aspects and Performance Indicators

Evaluation Aspect	Performance Indicator	References
Execution Speed	Contract response time < 2 seconds	Yatsenko et al. (2022); Ashtiani et al. (2024); Ambekar et al. (2024)
Cost Efficiency	Gas cost variation < 15% across scenarios	Yatsenko et al. (2022); Ashtiani et al. (2024)
Auditability	All transactions recorded immutably	Rossi (2021); Kovalenko et al. (2024); Dominguez et al. (2024)
Regulatory Compliance	Compliance with GDPR, PSD2, and related standards	Nakamura (2020); Weerapperuma (2025); Gaganov et al. (2024)
Contract Security	Free from critical bugs and vulnerabilities	Ibekwe et al. (2024); Virani & Kyada (2022); Elnara (2023)

This experiment is designed to simulate real-world conditions using a testnet environment, with emphasis on security aspects, system performance, and readiness for applicable regulatory frameworks.

h. Cross-Study Comparative Synthesis

Based on the ten analyzed articles, variations emerge in the approaches to smart contract utilization within the banking sector, particularly in terms of implementation objectives, technological platforms employed, evaluation methodologies, and regulatory scope. Broadly, the studies can be grouped into three main categories: (1) optimization of banking operational processes such as loan processing and trade finance; (2) enhancement of transaction security and transparency; and (3) development of blockchain-based system architectures for cross-institutional integration.

From a technological standpoint, the majority of studies employ Ethereum as the primary implementation platform due to its mature smart contract ecosystem. However, several recent studies have shifted toward permissioned blockchain platforms such as Hyperledger Fabric to better accommodate governance requirements and access control mechanisms within structured banking environments. This trend indicates a paradigm shift from public blockchain models toward hybrid or consortium blockchain architectures that are more compatible with financial sector regulations [19].

Regarding evaluation approaches, not all studies conducted empirical testing through experimental or performance simulations. Some research remains conceptual or proof-of-concept in nature, lacking in-depth quantitative measurements of throughput, latency, or scalability. Studies that performed performance testing report improvements in operational efficiency and reductions in manual intervention. Nevertheless, scalability limitations persist, particularly when transaction volumes approach those of large-scale financial institutions [6] [20].

From a regulatory and compliance perspective, only a portion of the reviewed articles explicitly address data protection issues, adherence to banking regulations, and the legal implications of digital contracts. Most studies emphasize technical efficiency, while systematic analysis of systemic risk and the potential consequences of smart contract failure within national financial systems remains limited. This gap reinforces the urgency of integrating technical innovation with risk governance frameworks in future research.

Overall, this comparative synthesis reveals that the existing literature remains fragmented between technical approaches and regulatory perspectives. Therefore, this study contributes by integrating technical analysis, regulatory compliance considerations, and systemic risk implications within a more comprehensive systematic review framework.

Table 5. Comparative Characteristics of Smart Contract Studies in Banking

No.	Authors	Study Focus	Platform / Technology	Blockchain Type	Evaluation Method	Regulatory Discussion
1	Dominguez et al.	Trade finance automation	Ethereum	Public	Proof-of-Concept	No
2	Ambekar et al.	Loan processing system	Ethereum	Public	Simulation	Limited
3	Khezr et al.	Fraud prevention	Hyperledger Fabric	Permissioned	Experimental evaluation	Yes
4	Alharby & van Moorsel	Smart contract security	Ethereum	Public	Security analysis	No
5	Zhang et al.	Interbank transactions	Hyperledger Fabric	Consortium	Performance testing	Limited
6	Xu et al.	Digital identity in banking	Ethereum	Public	Conceptual design	Yes
7	Chen et al.	Compliance monitoring	Hyperledger	Permissioned	Framework design	Yes

No.	Authors	Study Focus	Platform / Technology	Blockchain Type	Evaluation Method	Regulatory Discussion
8	Li et al.	Payment settlement	Ethereum	Public	Simulation	No
9	Singh et al.	Risk management	Consortium Blockchain	Consortium	Model analysis	Yes
10	Kumar et al.	Hybrid blockchain model	Hybrid (Public + Private)	Hybrid	System architecture design	Yes

i. Systemic Analysis and Implications

One of the primary paradoxes in implementing smart contracts within the banking sector lies in the conflict between the immutability principle of blockchain and data protection regulations, particularly the General Data Protection Regulation (GDPR). Blockchain technology is fundamentally designed to ensure that once data are recorded in the distributed ledger, they cannot be altered or removed. This characteristic guarantees a high level of data integrity, transparency, and traceability within financial transactions [11]. However, data protection regulations such as the GDPR grant individuals the legal right to request the deletion of their personal information, commonly referred to as the “right to be forgotten.” In banking environments where highly sensitive data such as identity credentials, financial records, and transaction histories are processed, this regulatory requirement becomes difficult to reconcile with blockchain’s immutable architecture.

If personal data are stored directly on the blockchain, deleting such data becomes technically infeasible because every node in the network maintains a synchronized copy of the ledger. Consequently, several technical solutions have been proposed to address this issue. One widely discussed approach involves off-chain data storage, in which sensitive personal information is stored outside the blockchain infrastructure, while only cryptographic hashes or verification references are recorded on-chain. Another strategy includes advanced encryption mechanisms that allow encrypted data to remain on the ledger but become inaccessible without the corresponding decryption keys. Although these approaches offer partial solutions, they introduce additional complexities in system architecture, governance models, and legal accountability frameworks [21].

Beyond regulatory concerns, system scalability represents another critical challenge. Large financial institutions process extremely high volumes of transactions daily and require near-instant processing speeds. Traditional banking infrastructures are optimized for high throughput through centralized database architectures. In contrast, public blockchain platforms such as Ethereum rely on distributed consensus mechanisms that inherently limit transaction throughput. As a result, large-scale smart contract deployment may experience higher latency, increased transaction fees, and reduced operational efficiency during periods of network congestion. This limitation raises questions regarding the readiness of current blockchain infrastructures to support global financial operations. Several studies suggest implementing layer-2 scaling solutions or adopting consortium-based blockchain architectures as potential mitigation strategies, although these approaches may reduce the degree of decentralization originally envisioned in blockchain systems [22].

To better understand the broader systemic implications of smart contract adoption in the banking sector, the following table summarizes key challenges and their potential impacts.

Table 6. Systemic Challenges in Smart Contract Adoption within Banking Systems

Systemic Dimension	Key Challenge	Potential Impact	Mitigation Strategy
Regulatory Compliance	Conflict between blockchain immutability and data protection laws (GDPR)	Legal uncertainty in handling personal financial data	Off-chain storage, encryption mechanisms, regulatory sandbox frameworks
Scalability and Performance	Limited transaction throughput in public blockchain systems	Delays in transaction processing during high-volume operations	Layer-2 scaling solutions and consortium blockchain models
Security Risks	Vulnerabilities in smart contract code such as reentrancy attacks or logic errors	Financial loss and operational disruption	Formal verification and automated security auditing
Governance and Accountability	Lack of centralized authority in decentralized systems	Difficulty in dispute resolution and liability determination	Consortium governance models and regulatory oversight

The framework presented in Table 6 highlights that the challenges of implementing smart contracts in banking are multidimensional, involving technical, regulatory, and governance-related considerations simultaneously. Regulatory compliance emerges as a major concern because financial institutions operate under strict supervisory frameworks that require accountability and consumer protection mechanisms. Without clear legal recognition of smart contracts, banks may face uncertainties in enforcing digital agreements within judicial systems [23].

Another critical issue involves security vulnerabilities in smart contract logic. Because smart contracts execute automatically once predefined conditions are met, any logical error embedded within the contract code may result in unintended financial consequences. Incidents such as reentrancy attacks or arithmetic overflow errors have previously demonstrated how vulnerabilities can be exploited to manipulate blockchain-based financial systems. In traditional banking systems, administrators may intervene to reverse transactions or suspend accounts. However, in blockchain environments, executed transactions are extremely difficult to reverse without significant network intervention such as protocol modification or hard forks [24]. Therefore, rigorous security audits, formal verification techniques, and multi-layer testing procedures must be conducted before deploying smart contracts within critical financial infrastructures [25].

Considering these limitations, many researchers propose the adoption of hybrid blockchain architectures as a practical compromise solution. Hybrid blockchain models combine the transparency and interoperability of public blockchains with the access control and efficiency of private networks. In such architectures, sensitive internal transactions are processed within permissioned networks controlled by participating banks, while cryptographic proofs or integrity hashes are anchored to public blockchains to maintain transparency and trust. This model is considered more compatible with regulatory requirements in the financial sector because it allows institutions to retain governance control while still benefiting from blockchain's core features.

Nevertheless, hybrid systems introduce new governance challenges related to interoperability standards, consortium management, and cross-institutional coordination. Without standardized protocols and clear governance frameworks, hybrid blockchain ecosystems may become fragmented and reduce the efficiency gains expected from distributed ledger technologies.

Overall, the systemic implications of smart contract adoption demonstrate that technological innovation alone is insufficient to transform banking infrastructures. Sustainable implementation requires an integrated approach involving technological engineering, cybersecurity governance, financial regulation, and institutional collaboration. Only through such multidisciplinary coordination can smart contracts evolve from experimental financial technologies into reliable components of the future digital banking ecosystem.

Conclusion

The utilization of smart contracts in banking offers transformative potential in redefining financial transaction processes. In terms of efficiency, security, and transparency, this technology provides substantial advantages. However, without proper technical risk mitigation and supportive regulatory frameworks, its full potential may not be realized. This study emphasizes the importance of a multidisciplinary approach in developing both technological infrastructures and policy frameworks to ensure safe and sustainable smart contract adoption.

Furthermore, the findings indicate that smart contract adoption in the banking sector cannot be separated from the readiness of supporting technologies such as blockchain infrastructure, oracles, and security auditing tools. Reliable system integration and adequate human resource training are critical determinants of long-term implementation success. Therefore, collaboration among technology developers, financial institutions, and regulators is essential to ensure that this innovation is not only technically effective, but also legally viable and socially acceptable.

Reference

[1] A. M. Ambekar, K. Anusha, M. K. Kumar, and A. K. Tyagi, "Smart Banking Solutions for Modern Society," in *Advances in Logistics, Operations, and Management Science*, 2024, pp. 98–110.

[2] F. Aprialim, "Penerapan Blockchain dengan Integrasi Smart Contract pada Sistem Crowdfunding," *Jurnal RESTI*, vol. 4, no. 2, pp. 215–220, 2020.

[3] S. M. Ashtiani, O. A. Adeli, M. Pourfakharan, and M. Maleki, "Futures Study of Smart Contracts in the Banking Industry," *Management Strategies and Engineering Sciences*, vol. 5, no. 4, pp. 201–210, 2024.

[4] J. A. Dominguez, S. Gonnet, and M. Vegetti, "The Role of Ontologies in Smart Contracts: A Systematic Literature Review," *Journal of Industrial Information Integration*, vol. 40, p. 100630, 2024.

[5] O. Elias, "The Evolution of Green Fintech: Leveraging AI and IoT for Sustainable Financial Services and

Smart Contract Implementation," *World Journal of Advanced Research and Reviews*, vol. 23, no. 1, pp. 2710–2723, 2024.

[6] S. Y. Gaganov, J. A. Dominguez, and M. Vegetti, "The Role of Ontologies in Smart Contracts: A Systematic Literature Review," *Journal of Industrial Information Integration*, vol. 40, p. 100630, 2024.

[7] Hasanah R, Prayitno HJ, Tuti S, Sarilan S, Prakoso V. Deep Learning-Based Learning Strategies in Realizing Meaningful, Critical, and Enjoyable Learning. Journal of Deep Learning. 2025.

[8] J. Huang, P. Li, Z. Chen, and Y. Wang, "Blockchain-Based Financial Applications: A Literature Review," *IEEE Access*, vol. 9, pp. 45678–45695, 2021.

[9] U. U. Ibekwe, U. Mbanaso, N. Nnanna, and U. A. Ibrahim, "Navigating the Smart Contract Threat Landscape," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 26, no. 3, pp. 455–462, 2024.

[10] Anggarini AG, Astuti E, Yusdita EE, Ulfatun T, Pascua RJ, Nafizah UY. Advancing accounting education: A Comprehensive Approach To Inventory Materials Learning Through Online Applications and The Smith-Ragan Model. *Indonesian Journal on Learning and Advanced Education (IJOLAE)*. 2024.

[11] V. N. Kollu, "Cloud-Based Smart Contract Analysis in FinTech Using IoT-Integrated Federated Learning in Intrusion Detection," *Data*, vol. 8, no. 5, p. 83, 2023.

[12] M. Krishnan, "Banking and Financial Contract Review (BaFiCoRe) Framework," *International Journal of Scientific Advances in Technology*, vol. 6, no. 1, pp. 12–19, 2025.

[13] T. Nakamura, "Smart Contracts and Legal Compliance in Financial Transactions," *Journal of Banking Regulation*, vol. 21, no. 3, pp. 310–327, 2020.

[14] Harmadi, Frisco, Ika Maryani, Sukirman Sukirman, and Elsa Carmen N. Montano. "Digital transformation: Exploring The Relationship Between Literacy, Motivation, and TPACK in Elementary Education." Indonesian Journal on Learning and Advanced Education (IJOLAE). 2025.

[15] E. S. Negara, "Survey of Smart Contract Framework and Its Application," *Information*, vol. 12, no. 7, p. 257, 2021.

[16] Y. Park and J. Lee, "Adoption Barriers of Smart Contracts in Banking Sector," *Asia Pacific Journal of Information Systems*, vol. 33, no. 1, pp. 45–67, 2023.

[17] C. S. Robusti, "Blockchain and Smart Contracts: Transforming Digital Entrepreneurial Finance and Venture Funding," *Journal of Small Business and Enterprise Development*, vol. 32, no. 2, pp. 210–227, 2025.

[18] A. Rossi, "Smart Contracts for Regulatory Compliance in Banking: A Framework," *International Journal of Law and IT*, vol. 29, no. 2, pp. 145–162, 2021.

[19] B. H. Susanto, M. N. Masrek, and I. E. Khairuddin, "Implementation of Smart Contract Technology in Financial Services Institutions," *Environment-Behaviour Proceedings Journal*, vol. 7, no. 21, pp. 23–29, 2022.

[20] H. Virani and M. Kyada, "A Systematic Literature Review on Smart Contracts Security," *arXiv preprint*, arXiv:2212.05099, 2022.

[21] U. S. Weerapperuma, "A Knowledge Framework for Blockchain-Enabled Smart Contract Adoption in the Construction Industry," *Engineering, Construction and Architectural Management*, vol. 32, no. 3, pp. 456–472, 2025.

[22] V. Yatsenko *et al.*, "Smart Contract in Banking for Ukraine's Economy Digitalization," *Vìsnik Sums'kogo deržavnogo unìversitetu*, no. 2, pp. 67–74, 2022.

[23] L. Zhang and M. Wei, "Smart Contracts in Banking: Opportunities and Risks," *Journal of Fintech Innovation*, vol. 3, pp. 112–126, 2022.

[24] A. Jufriansah, "NuminaMath 7B: Revolutionizing Math Solving with Integrated Reasoning Advanced Generative AI Tools and Python REPL", *saintek*, vol. 2, no. 1, pp. 1–19, Feb. 2026.

[25] D. R. Maulida, N. A. Suryaningtyas, S. Anggita, and U. Mahmudah, "Influence of Perceived Security and Perceived Risk on Continuance Intention in Using ShopeePay Digital Wallet Service: SEM-PLS Analysis", *saintek*, vol. 2, no. 1, pp. 44–57, Feb. 2026.