World Journal of Information Technology
Print ISSN: 2959-9903
Online ISSN: 2959-9911
DOI: https://doi.org/10.61784/wjit3063

SMART CONTRACTS: A COMPREHENSIVE SURVEY OF TECHNOLOGY, APPLICATIONS, AND CHALLENGES

RongHua Li[1*], Yun Li[1], XinMan Luo[2]
[1]*School of Finance and Economics, Hainan Vocational University of Science and Technology, Haikou 571126, Hainan, China.*
[2]*School of Information Science and Technology, Qiongtai Normal University, Haikou 570228, Hainan, China.*
[*]*Corresponding Author: RongHua Li*

Abstract: Smart contracts, as self-executing code on blockchain platforms, are transforming digital agreements across multiple industries. This paper reviews the technical foundations, applications, security challenges, and emerging directions of smart contract technology through an analysis of recent academic literature and real-world implementations. While smart contracts demonstrate significant potential in decentralized finance, supply chain management, and healthcare, they face critical challenges, including security vulnerabilities, ecosystem centralization risks, and legal uncertainties. Layer-2 scaling solutions, cross-chain interoperability protocols, and AI-assisted security auditing represent promising directions for addressing these challenges. Our analysis reveals that despite technological advances, fundamental issues in security verification and regulatory frameworks require continued research attention.
Keywords: Smart contracts; Blockchain; Decentralized finance; Security vulnerabilities

1 INTRODUCTION

Smart contracts are self-executing agreements with the terms directly written into code, which is stored on a blockchain-based platform [1]. Unlike traditional contracts that rely on human interpretation and enforcement mechanisms, smart contracts automatically execute predetermined actions when specific conditions are met [2]. These digital agreements represent a fundamental shift in how transactions and business processes are automated, offering advantages such as tamper-resistance, transparency, and the elimination of intermediaries. As a critical component of blockchain-based applications, a smart contract is "a digital contract that allows terms to depend on a decentralized consensus, is tamper-resistant, and is typically self-enforcing through automated execution" [3]. The significance of smart contracts lies in their ability to expand the contractual landscape through algorithmic execution while providing decentralized consensus. This technological innovation has garnered interest across multiple industries, from finance and supply chain to healthcare and energy, with implementations ranging from simple token transfers to complex decentralized applications.

This paper provides a comprehensive survey of smart contract technology, examining its technical foundations (Section 2), diverse applications across industries (Section 3), security vulnerabilities and systemic risks (Section 4), and emerging technological directions (Section 5). This survey distinguishes itself by integrating code-level security analysis with ecosystem-level centralization risks, providing researchers and practitioners with a holistic view of current challenges and future opportunities in smart contract development and deployment.

2 TECHNICAL FOUNDATIONS

A smart contract is computer code replicated across multiple blockchain nodes, ensuring security, permanence, and immutability through distributed consensus. Once deployed, the code executes automatically when transaction parameters meet predetermined conditions [1]. Most smart contracts are written in specialized programming languages; on Ethereum, which pioneered programmable smart contracts, Solidity dominates, though alternatives like Vyper exist [1, 4]. Unlike traditional legal documents requiring human interpretation, smart contract code directly specifies and automatically enforces rules and consequences through algorithmic execution.

2.1 Decentralized Consensus and Immutability

A defining feature of smart contracts is their reliance on decentralized consensus mechanisms. Unlike centralized systems where a single authority validates transactions, blockchain networks distribute this responsibility among multiple nodes. This decentralization prevents any single party from exercising market power and ensures that contract execution is not subject to the influence of a central authority [3]. The immutability of the blockchain ensures that once a smart contract is deployed, its code cannot be altered. This feature provides security and reliability but also presents challenges when contracts contain bugs or need to adapt to changing circumstances [5]. The tamper-resistant nature of smart contracts stems from their integration with blockchain technology, making them resistant to modification after deployment and confirmation by the network [6].

2.2 Contractibility and Automation

Smart contracts may reduce the scope of non-contractible contingencies that underpin the incomplete contracting literature in economics [7]. By enabling more precise and automated execution of contractual terms, smart contracts might increase the contractibility of certain conditions that were previously difficult to enforce, such as lock-in requirements for fund withdrawals or automated payments upon specific trigger events. The automation aspect of smart contracts represents one of their most valuable features. Once deployed, these contracts can execute without further human intervention, reducing administrative overhead and the potential for human error [8]. This self-executing property allows for more efficient and reliable transaction processing across various applications.

3 APPLICATIONS

Smart contracts demonstrate exceptional versatility, finding applications across numerous industries and use cases. Their ability to automate processes, reduce intermediaries, and ensure transparent transactions has driven adoption in various sectors.

3.1 Finance and Decentralized Finance (DeFi)

The financial sector has been at the forefront of smart contract adoption through Decentralized Finance (DeFi), where automated lending, decentralized exchanges, and yield farming operate without traditional intermediaries [3]. These applications enable users to manage cryptocurrency assets through programmatic rules, creating financial primitives impossible in conventional systems [9]. However, the high-value nature of DeFi makes it a prime attack target. However, financial applications of smart contracts have also become prime targets for attacks. Notable incidents include the 2016 DAO attack (resulting in a $50 million loss), the 2017 Parity wallet hack ($146 million locked), the 2018 Beautychain (BEC) token incident (market cap dropping from $900 million to zero), and a 2022 NFT gaming blockchain breach ($600 million stolen) [4]. Collectively, these incidents reveal that financial smart contracts face disproportionate security risks, with losses far exceeding those in other application domains—a pattern that persists despite advances in auditing tools.

3.2 Supply Chain Management

Smart contracts enhance supply chain management by increasing transparency, reducing paperwork, and automating payments based on verifiable events. They enable stakeholders—suppliers, manufacturers, distributors, and retailers—to interact without central authority oversight, creating a trustless system. For instance, a smart contract can automatically release payment once IoT devices confirm goods arrival under specified conditions, reducing delays, disputes, and administrative costs while maintaining tamper-proof records [10].

3.3 Healthcare

Applications of smart contracts in healthcare focus on improving data management, patient privacy, and research integrity. Smart contracts can facilitate the secure sharing of medical records while giving patients control over who can access their information. They also enable more transparent clinical trials by recording protocols, consent, and results on an immutable ledger [10]. Implementing blockchain-based smart contracts in healthcare can address challenges related to data interoperability, consent management, and research reproducibility, ultimately improving patient outcomes and reducing administrative burdens [6].

3.4 Public Administration and Governance

Smart contracts are being explored for various public administration functions, including voting systems, property registries, and government procurement processes [10]. These applications aim to increase transparency, reduce corruption, and improve the efficiency of public services. For instance, a blockchain-based voting system using smart contracts could provide a verifiable and tamper-proof record of votes while maintaining voter privacy [10]. Similarly, land registries implemented with smart contracts could reduce fraud and administrative costs in property transactions.

4 SECURITY AND LIMITATIONS

Despite their potential benefits, smart contracts face significant security challenges and limitations that must be addressed for wider adoption. These include technical vulnerabilities, legal complexities, and practical implementation challenges.

4.1 Technical Vulnerabilities

Smart contracts are susceptible to various vulnerabilities that can lead to significant financial losses. Common vulnerabilities include re-entrancy attacks, overflow/underflow errors, front-running, and access control issues [4]. The immutable nature of the blockchain means that once deployed, vulnerable contracts are not easily fixed, highlighting the

critical importance of thorough testing and auditing before deployment. An analysis of 127 high-impact real-world attacks resulting in $2.3 billion in losses found that current automatic security tools could only prevent 8% of these attacks, corresponding to just $149 million in potential savings [9]. Notably, all preventable attacks were related to re-entrancy vulnerabilities, indicating the limitations of existing security tools in addressing the full spectrum of smart contract vulnerabilities. Furthermore, practitioners identify logic-related bugs and protocol-layer vulnerabilities as significant threats that existing security tools do not adequately address [9]. This gap between security tool capabilities and developer needs represents a significant challenge for the industry.

4.2 Contract Dependencies and Centralization Risks

A large-scale empirical study of over 41 million contracts and 11 billion interactions on Ethereum revealed worrying patterns regarding smart contract dependencies. The study found that 59% of contract transactions involve multiple contracts (with a median of 4 per transaction in 2024), indicating significant smart contract dependency risk [11]. More alarmingly, the ecosystem exhibits extreme centralization, with just 11 deployers (0.001%) controlling 20.5 million (50%) of all active contracts. This centralization creates significant risks related to factory contracts and deployer privileges [11]. Furthermore, the three most-depended-upon contracts are mutable, meaning a large portion of the ecosystem relies on contracts that can be changed at any time, creating substantial systemic risk. The research also found that actual smart contract protocol dependencies are far more complex than documented in official repositories, which compromises Ethereum's transparency philosophy and creates unnecessary attack surfaces. These findings challenge the notion of decentralization commonly associated with blockchain technology.

4.3 Legal and Regulatory Challenges

Smart contracts face significant legal and regulatory challenges. First, jurisdictional ambiguity arises from blockchain's decentralized nature—when disputes occur in cross-border smart contracts, determining applicable legal frameworks remains unresolved. Second, traditional legal systems may not recognize code-based contracts as legally binding, creating uncertainty about enforceability when contracts fail or malfunction. Third, liability attribution becomes complex when code bugs cause unintended consequences, as responsibility may lie with platforms, developers, or contracting parties, unlike traditional contracts where accountability is typically clear [2]. These legal uncertainties hinder mainstream adoption and highlight the need for updated regulatory frameworks that accommodate automated, code-based agreements.

5 EMERGING TRENDS

In response to the security, scalability, and interoperability challenges identified above, the smart contract ecosystem is evolving through several technological innovations. This section examines three primary directions—Layer-2 scaling, cross-chain interoperability, and AI integration—that collectively address current limitations while expanding the functional capabilities of blockchain-based applications.

5.1 Layer-2 Scaling Solutions

Layer-2 (L2) scaling solutions represent one of the most significant developments in smart contract technology, addressing critical challenges of scalability, transaction speed, and cost. These solutions act as secondary frameworks built on top of a Layer-1 blockchain like Ethereum, processing transactions more efficiently off-chain to alleviate the computational burden on the main chain. Popular L2 approaches include Rollups (both Optimistic and ZK-Rollups), state channels, sidechains, and Plasma [12-13]. Rollups batch transactions off-chain and submit a summary to the main chain for verification, while state channels facilitate direct peer-to-peer interactions, using the main chain only for dispute resolution. Empirical evidence demonstrates the effectiveness of these scaling solutions: a study on L2 technologies found they reduced operational costs by 76% while fostering decentralization by lowering market concentration and increasing participation, which in turn improved data accuracy [14]. However, as with any technological innovation, L2 solutions introduce trade-offs, such as increased complexity in cross-layer communication and potential security risks in the bridging mechanisms [7].

5.2 Cross-Chain Interoperability

Cross-chain smart contracts represent another significant trend, addressing the limitations of single-blockchain environments. These applications consist of multiple smart contracts deployed on different blockchain networks that interoperate to create unified applications, leveraging the unique strengths of different blockchains, sidechains, and L2 networks [15]. The rise of the multi-chain ecosystem has been driven by the demand for low-cost alternatives to the Ethereum mainnet while maintaining security and functionality. Cross-chain interoperability protocols, such as the Cross-Chain Interoperability Protocol (CCIP), facilitate secure communication between blockchains, enabling more complex and efficient applications that were previously not possible. This development represents a paradigm shift in how decentralized applications are architected. Yet, it also introduces new attack surfaces, as security must be

maintained across multiple, potentially heterogeneous chains, and the trust assumptions of cross-chain bridges remain a topic of ongoing research [7].

5.3 Integration of AI and Smart Contracts

The integration of Artificial Intelligence (AI) with smart contracts represents one of the most transformative emerging trends. AI-powered smart contracts go beyond traditional automation by incorporating advanced decision-making, pattern recognition, and adaptive capabilities [8]. While standard smart contracts execute fixed rules, AI-driven contracts can adapt and learn from new data, making them more versatile and intelligent. This fusion of AI and smart contracts is transforming industries from DeFi to supply chain, offering smarter, faster, and more scalable solutions. For example, in DeFi, AI-enhanced smart contracts can analyze market trends to optimize lending rates or implement more sophisticated risk management strategies, potentially addressing some of the financial inefficiencies discussed in prior research [3]. Another emerging application involves the use of Large Language Models (LLMs) for Solidity vulnerability detection. Research has shown that models like GPT-3.5 Turbo and GPT-4o Mini, after fine-tuning, achieve 99% accuracy in detecting vulnerabilities, 94% in type identification, and 98% in severity determination [4]. However, this integration raises new questions about the verifiability and predictability of AI-driven decisions on an immutable ledger, as the dynamic nature of AI may conflict with the deterministic requirements of blockchain systems.

6 CONCLUSION

his survey illustrates that smart contracts are at a pivotal stage of development. While their applications in finance, supply chain, and other sectors continue to expand, their foundational promises of decentralization and security are being tested by persistent and evolving challenges. Our analysis highlights a core tension: at the code level, vulnerabilities remain a critical threat, with empirical evidence demonstrating that automated security tools prove insufficient against the majority of real-world attacks. Simultaneously, at the ecosystem level, the smart contract landscape exhibits significant centralization, where recent large-scale studies reveal that a small number of deployers control a vast portion of deployed contracts, creating systemic risks that contradict the technology's decentralized ethos. Emerging trends such as Layer-2 scaling, cross-chain interoperability, and AI integration offer promising pathways to address these limitations. However, they also introduce new layers of complexity and risk, including cross-layer communication challenges, trust assumptions in bridging mechanisms, and the tension between AI's dynamic nature and blockchain's deterministic requirements. Based on these findings, we propose three critical future research directions: (1) developing next-generation security tools that move beyond pattern matching to address logic-related bugs and protocol -layer vulnerabilities; (2) establishing standards and governance frameworks for managing cross-contract dependencies to mitigate systemic centralization risks; and (3) creating verifiable and explainable AI models suitable for integration with immutable ledger technologies. Addressing these areas is crucial for realizing the transformative potential of smart contracts while maintaining their core properties of security, decentralization, and trustlessness.

COMPETING INTERESTS

The authors have no relevant financial or non-financial interests to disclose.

FUNDING

This article is the Scientific Research Project of Higher Education Institutions in Hainan Province in 2025: Research on the Driving Mechanism and Realisation Path of the High-quality Development of Hainan's Advanced Manufacturing Industry under the New Pattern of Double-cycle Development (Project No. Hnky2025-63).

REFERENCES

[1] Levi SD, Lipton AB. An Introduction to Smart Contracts and Their Potential and Inherent Limitations. Harvard Law School Forum on Corporate Governance, 2018. https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/.
[2] Ballaji N. Smart Contracts: Legal Implications in the Age of Automation. Beijing Law Review, 2024, 15(3): 1015.
[3] Cong LW, He Z. Blockchain disruption and smart contracts. The Review of Financial Studies, 2019, 32(5): 1754-1797.
[4] Alam MT, Halder R, Maiti A. Detection Made Easy: Potentials of Large Language Models for Solidity Vulnerabilities. arxiv preprint arxiv:2409.10574, 2024.
[5] Aladağ H, Güven İ. Risk factors affecting blockchain-based smart contract use in architecture, engineering, and construction industry. Megaron, 2023, 18(2).
[6] Zheng X. Research on blockchain smart contract technology based on resistance to quantum computing attacks. Plos one, 2024, 19(5): e0302325.
[7] Taherdoost H. Smart contracts in blockchain technology: A critical review. Information, 2023, 14(2): 117.
[8] Komodo Platform. AI Smart Contracts: What Are They and How Do They Work? 2025. https://komodoplatform.com/en/academy/ai-smart-contracts/.

[9] Chaliasos S, Charalambous MA, Zhou L, et al. Smart contract and defi security tools: Do they meet the needs of practitioners?. Proceedings of the 46th IEEE/ACM International Conference on Software Engineering, 2024.
[10] Xu Y, Chong HY, Chi M. A review of smart contracts applications in various industries: a procurement perspective. Advances in Civil Engineering, 2021, 2021(1): 5530755.
[11] Jin M, Liu R, Monperrus M. On-Chain Analysis of Smart Contract Dependency Risks on Ethereum. arxiv preprint arxiv:2503.19548, 2025.
[12] Metana. Layer 2 Smart Contracts: Opportunities and Challenges. 2025. https://metana.io/blog/layer-2-smart-contracts-opportunities-and-challenges/.
[13] Zent. Introduction to Layer-2 smart contracts. 2024. https://zent.pro/blog/introduction-to-layer-2-smart-contracts.
[14] Cong LW, Hui X, Tucker C, et al. Scaling smart contracts via layer-2 technologies: Some empirical evidence. Management Science, 2023, 69(12): 7306-7316.
[15] Chainlink. What Are Cross-Chain Smart Contracts? 2023. https://chain.link/education-hub/cross-chain-smart-contracts.