Research on Legal Issues of Smart Contract Architecture

Hongxin Hu
School of Law (School of Intellectual Property), China Jiliang University, Hangzhou, Zhejiang, China

Abstract: In the context of economic globalization and rapid internet development, emerging digital technologies such as cloud computing, big data, and AI are revolutionizing industry production and sales. Smart Contracts, particularly empowered by blockchain advancements, present promising prospects. However, traditional contracts remain dominant in economic activities, especially in China's vast SME market, where risks of real world transaction instability hinder smart contract adoption. Technical vulnerabilities and ecological security issues in smart contract platforms pose challenges in translating legal language into code. Despite progress in natural language processing, translating legal documents accurately remains difficult, burdening judges and programmers with time costs. Therefore, research on smart contract architecture and legal applications, along with practical solutions, is imperative for both theoretical and practical advancements.

Keywords: Smart Contracts; Smart Contract Architecture; Legal Issues

1. Introduction

Smart Contracts represent a pivotal application of blockchain technology, demonstrating significant potential to transform sectors such as finance, supply chain management, and real estate. Their core value propositions—automation, tamper-resistance, and decentralization—offer substantial efficiency gains by reducing reliance on intermediaries, minimizing the potential for manual error or fraud, and accelerating transaction speeds. By executing predefined terms automatically upon the fulfillment of specific conditions, they promise a new paradigm of trustless and transparent agreement enforcement. [1] However, the implementation of smart contracts confronts a complex array of legal and practical challenges that extend beyond their technical execution. While they ensure the performance of coded terms, significant disputes can arise concerning liability allocation when code behaves unexpectedly, the interpretation of parties' true intentions versus the rigid code output, and the reconciliation of blockchain's inherent transparency with stringent data protection regulations like the GDPR. The very features that make smart contracts powerful—decentralization and immutability—also create friction with established legal principles that allow for contract modification, revocation under certain conditions (e.g., mistake, fraud, or duress), and flexibility in the face of unforeseen events (force majeure). Addressing these issues requires a concerted interdisciplinary collaboration between legal scholars, practitioners, and technical experts. The goal is to align the innovative capabilities of smart contracts with the protective and interpretative functions of existing legal frameworks. This study aims to systematically analyze the architecture of smart contracts, identifying specific legal pitfalls embedded within their technical layers. By examining these challenges from the perspective of civil law systems, particularly China's Civil Code, and broader regulatory concerns like data protection, this research seeks to propose actionable, practical solutions. The ultimate objective is to facilitate the credible, secure, and sustainable adoption of smart contracts, enabling them to realize their full potential as a cornerstone of the digital economy.[2]

2. Overview of Smart Contract Architecture

The concept of "Smart Contracts" was first proposed by computer scientist and cryptographer Nick Szabo in 1994. He famously analogized them to digital vending machines: autonomous mechanisms that, upon receiving a predefined input (e.g., currency), automatically perform a predefined output (e.g., dispensing a

product) without requiring a trusted third party. This foundational idea has found its most robust realization through blockchain technology. At their core, smart contracts are self-executing programs stored on a blockchain. They differ fundamentally from traditional contracts by automating the execution phase through code.[3] Key distinguishing features include: Decentralization, Execution is not controlled by a single entity but is distributed across a network of nodes, reducing single points of failure and control. Transparency: The contract code and, in many cases, the transaction history are visible to participants, fostering trust through verifiability. Immutability: Once deployed to a blockchain, the contract code is extremely difficult to alter, ensuring that the agreed-upon rules cannot be changed arbitrarily. Efficiency: Automation eliminates manual processing, intermediary delays, and associated costs, leading to faster and cheaper execution. Smart contracts rely on the underlying blockchain's distributed ledger system. When a transaction invoking a smart contract is initiated, it is broadcast to the network. Nodes (miners or validators) then validate the transaction and execute the code according to the consensus algorithm (e.g., Proof of Work, Proof of Stake). The result of this execution is then recorded immutably on the blockchain. The code, often written in specialized programming languages like Solidity (for Ethereum) or Vyper, runs within a Virtual Machine (VM) on the blockchain, providing a sandboxed environment for execution. [4] The applications are vast and transformative. In healthcare, they can manage patient data access permissions; in finance, they power decentralized finance (DeFi) applications like lending and trading; in supply chains, they can automatically trigger payments upon theverified delivery of goods. For instance, integrating smart contracts into large-scale engineering projects—such as through a Building Information Modeling (BIM) platform like BIMWAY—could streamline procurement, automate milestone-based payments, mitigate costly payment disputes, and enhance overall project transparency for all stakeholders. However, a critical challenge arises from the rigidity of smart contracts, which contrasts sharply with the inherent flexibility of traditional contracts. Modifications or terminations after deployment are complex and often require deploying a new contract, posing significant risks if undiscovered vulnerabilities exist in the original code. This rigidity is a double-edged sword, providing certainty but lacking the nuance and adaptability of natural language agreements interpreted within a flexible legal framework.[5]

2.1 Architecture Components

The architecture of a smart contract system can be deconstructed into interconnected technical and legal layers.

2.1.1 Technical Layers

It can be divided into four levels, first one is System Layer, OS, network protocols, databases. The secend is Contract Layer: Logic code (Solidity/Vyper) defining terms and triggers. The next is Invocation Layer: Interfaces for user interaction (APIs, web apps). Last one is Blockchain Network: Consensus mechanisms (e.g., Ethereum, Hyperledger ensure validity.

2.1.2 Legal Considerations Embedded in Architecture

The technical architecture directly implicates several fundamental legal concepts: Contract Formation, Traditional contract law requires a clear offer, acceptance, and consideration. In smart contracts, "consensus" is achieved differently. The offer may be embedded in the code, and acceptance occurs through a user's interaction (e.g., signing a transaction with a private key). This interaction is then verified by miners, creating a binding agreement. The immutability of this recorded "acceptance" challenges traditional notions of revocability before acceptance is communicated. The next one Execution vs. Ownership Transfer: In many civil law systems, including China's, there is a principle of separation between the underlying obligation (the contract) and the disposition of property (the transfer of ownership). A sales contract creates an obligation to transfer ownership, but the actual transfer is a separate legal act. Smart contracts, however, can be programmed to autonomously execute both the contractual obligation and the transfer of a digital asset (e.g., a token representing ownership) simultaneously. This conflation can blur important legal boundaries and create uncertainty in complex transactions involving physical assets. The Intent Verification means the automated, literal execution of code risks misinterpreting or failing to capture the parties' true, subjective intentions, especially in complex or nuanced agreements. If the code does not

accurately reflect the meeting of the minds (consensus ad idem), the rigid execution can lead to outcomes that a court would deem unfair or invalid under traditional contract law principles. For instance, consider the most typical sales contract. When the buyer and seller reach an agreement, the contract becomes effective without actual delivery. However, the transfer of property rights requires physical delivery or ownership registration. In smart contracts, when parties establish a clause that automatically executes upon meeting conditions—such as transferring funds to the seller's account—the subject matter of the contract immediately transfers to the buyer, directly making the contract effective and triggering property rights changes. This reduces disputes and resolves creditor's rights disputes at the source. China's legislative model for property rights transfer generally holds that creditor contracts like sales and gifts alone are insufficient to cause property rights changes; registration or delivery must also occur for legal effect. Unregistered or undelivered actions do not affect the validity of creditor contracts. Even if a creditor contract is revoked or declared invalid, property rights remain unchanged. This is known as the "distinguishing principle," which aims to differentiate property rights from creditor's rights. The claim rights of creditor contracts differ from the control rights of property rights, meaning changes in creditor's rights alone cannot alter property rights. For example, when a seller sells a cow to a buyer who pays and receives the animal, if the buyer defaults on payment, the seller can only claim the money rather than directly purchasing the cow from the buyer. This has led some researchers to question: Why can't the original property rights holder exercise control rights after becoming a creditor in civil acts like sales that transfer property rights? In China's legal theory circles, such transactions are generally defined as creditor's rights acts involving tangible assets. This refers to the act where a property owner sells their possession to a buyer to obtain creditor's rights. As a claim right, creditor's rights can only demand performance from the party involved, not the delivery of the original or specific property. When property rights transfer through sales contracts, the original owner gains creditor's rights while losing property rights. If the seller neither physically delivered the cattle to the buyer nor was in good faith in acquiring the cattle (through possession modification), the seller retains ownership. If the contract grants the seller a first-strike defense, the buyer must pay the price before demanding delivery. In comparison, smart contracts' conditions or code cannot establish such flexible dual procedures for property and creditor's rights. However, precisely this undifferentiated setup facilitates dispute resolution.[6]

2.1.3 Legal Challenges in Smart Contract Architecture

The integration of smart contracts into the legal landscape raises profound questions that can be analyzed from both civil code perspectives and broader regulatory standpoints. In accordance with China's relevant legislation, while electronic contracts hold the same legal validity as written contracts, special electronic agreements like smart contracts require reasonable regulation. [7] These should be governed similarly to administrative contracts requiring approval or civil contracts involving sensitive matters, such as infrastructure projects affecting public welfare. By establishing binding conditions and ensuring full documentation from contract drafting to execution on designated platforms, we can achieve pre-approval, real-time tracking, and post-implementation filing to maximize smart contract benefits. While the vision is promising, China currently lacks the necessary technological infrastructure. Challenges persist in code development, vulnerability remediation, and the broader data ecosystem, all of which demand urgent attention. The first is Civil Code Perspectives, it is further divided into three categories: Contract Validity, Jurisdiction and Dispute Resolution, Interpretation and Amendments. The following section will provide a detailed discussion.

The validity of a smart contract under a civil code is not automatic. Issues arise if the code-based terms are ambiguous, incomplete, or violate public order and good morals. A more significant challenge is fraudulent contracts. Malicious actors could exploit coding loopholes or create contracts with hidden, unfavorable terms that are difficult for a non-technical party to discern, challenging the determination of validity based on genuine consent. The decentralized and borderless nature of blockchain complicates the assignment of jurisdiction. If parties are in different countries

and the contract executes on a global network, which court has authority? China's developing system of internet courts may need to adapt specialized rules and technical capabilities to effectively handle cross-border smart contract disputes. When a dispute arises, courts are faced with the task of interpreting code. This often requires the assistance of technical experts, adding cost and complexity. Furthermore, smart contracts frequently use predefined template clauses. These standardized terms risk non-compliance with contract law provisions that regulate standard form contracts, such as those in Articles 496-497 of China's Civil Code, which require promoters to draw attention to exclusion or limitation clauses and interpret ambiguities against the party providing the terms. The secend is Data Protection, Enforcement, and Regulation, it is also divided into four categories: Privacy vs. Transparency, Regulatory Compliance, Force Majeure Handling and Execution Risks A fundamental tension exists between blockchain's transparency and data protection laws like China's Personal Information Protection Law (PIPL) and the EU's GDPR. Storing personal data on a public, immutable ledger can conflict with the "right to be forgotten" or data rectification. Additionally, intellectual property rights surrounding the code itself can lead to ownership disputes, especially in open-source environments. Smart contracts used in regulated industries like finance (e.g., for tokenized securities or insurance payouts) must adhere to stringent know-your-customer (KYC), anti-money laundering (AML), and securities regulations. Ensuring that an automated, decentralized contract complies with these evolving rules is a major hurdle.[8]

Traditional contracts have doctrines to handle unforeseen, unavoidable events that make performance impossible or impracticable. An automated smart contract lacks the cognitive ability to recognize such events and suspend or adjust performance, potentially leading to unfair outcomes. Technical flaws in contract code can lead to catastrophic losses, as exemplified by the 2016 DAO hack where millions of dollars were drained due to a reentrancy vulnerability. This highlights the critical need for robust, independent security auditing and potentially introducing mechanisms for pausing or upgrading contracts in emergencies. Conclusion As a cornerstone of Web3.0 and IoT, smart contracts' success hinges on reconciling technical innovation with legal certainty. China's unique market dynamics demand tailored solutions balancing efficiency with risk mitigation. Future advancements require interdisciplinary collaboration to establish clear legal standards, robust technical protocols, and user friendly platforms. By addressing current challenges, smart contracts can revolutionize transactions across sectors, enhancing trust and efficiency.[9]

3. Improving Smart Contract Architecture: A Multifaceted Approach

To overcome these challenges and build a trustworthy ecosystem for smart contracts, a multi-pronged approach involving legal, technical, and governance enhancements is necessary. First of all, the legal framework should be improved. The most critical step is the development of a clear and supportive legal framework. This involves: Enacting Specialized Regulations and Establishing a Registration/Recording System. Legislatures should enact laws or regulations that explicitly recognize smart contracts as a valid form of contract, while defining the criteria for their validity. These regulations should clarify issues of jurisdiction, evidence rules for code, and the legal status of on-chain records. For high-risk sectors like construction and finance, mandatory registration or filing of smart contract code with a designated authority (e.g., a national blockchain registry) could enhance oversight, provide a clear record for dispute resolution, and allow for pre-deployment compliance checks. Secondly, it is urgent to improve the internal governance mechanism. Smart contracts themselves can be designed with more sophisticated internal governance to mitigate risks, for example, implementing a multi-signature approval system, AI-powered compliance checks, and upgradable contract templates. For critical actions (e.g., transferring large sums), the contract can require multiple private keys to sign off, preventing unilateral action and reducing the risk of theft or error. Integrating AI tools during the contract drafting phase can automatically flag terms that may be non-compliant with relevant regulations or identify common coding patterns associated with vulnerabilities. Using specific coding patterns that separate a contract's logic from its data storage, allowing for logic to be updated in

a controlled manner without losing critical data, can introduce necessary flexibility while maintaining security.[10]

Third, we should improve the platform's ability to resist risks. Platforms hosting or facilitating smart contracts have a role to play in fostering a secure environment: Participant Verification and Integrated Risk Assessment Tools. Platforms should perform background checks on participants, including credit history and litigation records, to build a reputation system and flag high-risk counterparties. The development of tools that can analyze contract terms and code to assess and flag potentially risky or suspicious clauses forusers before they commit. The fourth is to focus on the development of integrated platforms. The future lies in developing end-to-end platforms that seamlessly integrate the entire contract lifecycle. Like Unified Management Platforms: These platforms would combine smart contract drafting tools (with legal templates), execution monitoring dashboards, automated regulatory compliance reporting, and integrated dispute resolution modules (e.g., connecting to online arbitration services). Example - Government-Backed Construction Platform: A practical example would be a government-backed platform for public infrastructure projects. This platform could integrate smart contracts for automatic payment upon verified project milestones, BIM data for real-time supervision, and a built-in dispute resolution mechanism, thereby enhancing efficiency, transparency, and accountability. The end is to build a Full-process platform.[11] The construction of a management information system platform focuses on scientific and standardized management. By systematically streamlining and optimizing contract management processes, we have developed an intelligent management platform designed to serve as a smart contract execution tool, similar to payment platforms like Alipay.[12] With user-friendly operations accessible via desktop or mobile devices, the platform enables online contract submission, signing, execution, and real-time updates. It facilitates offline contract-related procedures such as "delivery," ownership transfer, and administrative approvals, while providing digital signatures, comprehensive free contract templates, automated contract execution programs, and streamlined payment flows through instant payments. This significantly enhances both contract management efficiency and transactional productivity. The system integrates legal regulations and policy provisions into its operational workflows, connecting backend data with internal contract management systems and operational platforms. For government agencies, multi-department collaboration on this platform eliminates the need for cross-regional travel, enables real-time contract tracking, and achieves seamless integration of digitalization, transactions, and research. This improves contract quality, controls transaction risks, and safeguards stakeholders' economic interests. Courts and public security bureaus can implement full-process oversight through smart contracts on this platform. When disputes arise, they can access recorded evidence materials, reducing litigation costs and streamlining case handling for judicial authorities. As a new approach to managing the entire development cycle of smart contracts, this platform maximizes regulatory oversight across government departments, balancing efficiency with security while simplifying administrative processes for national authorities.[13]

4. Conclusion

As a cornerstone of emerging technologies like Web3.0 and the Internet of Things (IoT), the success of smart contracts hinges on the successful reconciliation of technical innovation with legal certainty and user protection. China's unique market dynamics, characterized by a vast SME sector and a rapidly digitizing economy, demand tailored solutions that carefully balance the efficiency gains of automation with robust risk mitigation strategies. Future advancements will inevitably require deep interdisciplinary collaboration. Legal scholars must deepen their understanding of blockchain technology, while engineers must design systems with legal principles in mind from the outset. By establishing clear legal standards, developing robust and auditable technical protocols, and building user-friendly platforms that integrate legal and technical functions, the current challenges can be addressed. Through these efforts, smart contracts can truly revolutionize transactional paradigms across numerous sectors, ultimately enhancing trust, reducing costs, and fostering a more efficient and secure global digital economy.

Acknowledgments

This research was conducted under the university-level project of "Intelligent Contract: A New Approach to the Whole Process Management of Development". I would like to express my gratitude to Professor Che for his support and the data access provided by the laboratory.

References

[1] Szabo, N. (2018). Smart Contracts: Building Blocks for Digital Markets. Journal of Digital Markets, 1, 1-11.

[2] Chen, J. (2019). Legal Construction of Smart Contracts. East China Law Science, (03), 18-29.

[3] Xia, Q. (2022). Analysis on Legal Nature of Smart Contracts. East China Law Science, (06), 33-43.

[4] Ouyang, L., Wang S., Yuan Y., Xiaochun N., Wang F. (2019). Smart Contracts: Architecture and Advances. Acta Automatica Sinica, 45(03), 445-457.

[5] Ni, Y. (2019). Civil Law Analysis and Implications of Smart Contracts. Journal of Chongqing University (Social Science Edition), 25(03), 170-181.

[6] Wang, L. (2022). The Principle of Separation Under Formalism of Obligation. Tsinghua Law Journal, 16(03), 5-19.

[7] Chen, Y. (2018). Identification of Intentions in Smart Contracts. Hainan Finance, (05), 39-45.

[8] Cheng, L. (2022). Construction Path of Smart Contract Terms. Law Review, 40(02), 53-66.

[9] Cao, S. (2023). Normative Effects and Practical Optimization of Blockchain Smart Legal Contracts. Science, Technology and Law, (03), 108-115.

[10] Li, M. (2023). Risk Assessment and Legal Regulation of Smart Contracts. Academic Exchange, (03), 42-59.

[11] Jin, L. (2020). Risk Analysis and Legal Regulation of Blockchain Technology. Law Science Magazine, 41(07), 84-93.

[12] Yan, C. (2019). Construction and Risk Prevention of Smart Contracts. Law Science Magazine, (2), 43-51.

[13] Zhang, T. (2020). Legal Attributes and Risk Management of Smart Contracts. Cyberspace Security, 11(09), 47-54.

