



Regulating Smart Contract Applications in China: How to Strike a Balance between Innovation and Compliance?

Junlin Yi* and Zheheng Miao

KoGuan School of Law, Shanghai Jiao Tong University, Shanghai, 200030, China

*yijunlin_sjtu@126.com, miaozheheng@163.com

Abstract. Smart contract technology has revolutionized sectors like finance and supply chain management through its automated execution and decentralized nature in China. However, its rapid adoption necessitates robust regulatory frameworks to curb risks such as illegal activities and security vulnerabilities. A comparative analysis of international regulatory approaches reveals divergent policy priorities: the EU emphasizes personal data protection, the US fosters innovation in digital assets, Japan prioritizes transactional safety, South Korea safeguards investor rights, and the UK leverages regulatory sandboxes to balance innovation with control. This paper proposes a hybrid framework of community self-governance and indirect regulation to better mitigate risks while fostering the sustainable development of smart contract applications in China. A hierarchical evaluation system is also introduced, encompassing ex-ante review, interim monitoring, and ex-post audit, supported by quantifiable metrics to enhance regulatory efficacy.

Keywords: Smart Contract, Regulation, Virtual Community

1 Introduction

In the past few years, smart contracts have brought revolutionary changes to various fields such as finance, supply chain management, and copyright protection.[1] Built on top of the blockchain technology, a “smart contract” is a contract enshrined in machine-executable code. Once a smart contract is deployed on the blockchain, it will automatically execute the obligations that the parties have undertaken in the agreement, obviating the need for direct human intervention. Therefore, computer programs can render contractual relationships in a more efficient and economical manner, with potentially fewer occasions for error, delay, or dispute.[2]

While smart contract applications bring about numerous benefits, they also lead to significant illegal activities, such as money laundering and fraud.[3] There are legal risks surrounding this new technology that need to be addressed, which can be classified into the following types: (1) risks related to the infringement of rights, including infringing privacy, personal information and virtual property rights; (2) risks related to

legal applicability, concerning defects in contract validity, manifestation of intent, and the uncertainty of parties' rights to defense; (3) risks related to the inability to obtain effective remedies, such as the limited capacity to pursue liability for breach of contract; and (4) risks arising from accountability gaps, including risks due to the absence of regulation for illegal transactions and risks involving obstacles to the attribution of legal liability.

Therefore, the importance of regulatory compliance has become more and more prominent. Without proper regulation, malicious actors might exploit smart contract technology for money laundering, tax evasion, and other illegal activities, disrupting the stability of the market. Also, the legal regulation of smart contract applications helps protect the rights of users. Considering that the automatic execution of the smart contract applications is generally irreversible, any vulnerabilities at the code level might lead to irreparable losses. Therefore, ensuring the compliance of smart contract applications with the existing legal framework is of great significance.

The regulatory compliance of smart contract applications is a non-trivial issue. From a technical perspective, smart contract code should undergo rigorous auditing and testing to ensure security and reliability. This includes reviewing the static logic of smart contract applications to prevent potential software vulnerabilities; furthermore, runtime execution shall be monitored to ensure that applications actually operate according to the predefined logic. Therefore, it is necessary to create a comprehensive regulatory framework covering the development, deployment, and execution of smart contract applications.

Accordingly, the main research question of this paper is how to strike a balance between innovation and compliance for the regulation of smart contract applications in China. Specifically, regulators should take into account the following difficulties and challenges. First, smart contracts execute without a central authority, making traditional legal jurisdictions difficult to apply to this new paradigm. Second, the "Code is Law" philosophy of smart contract technology conflicts with traditional legal interpretation and application. The forced execution feature of smart contracts challenges fundamental principles of contract law.

2 Comparative Analysis of Smart Contract Application Regulation in Other Countries

The regulation of smart contract applications is an emerging issue in recent years, but a series of mechanisms related to it have been formed by different countries and regions. Through comparative analysis of the corresponding regulatory mechanisms in different countries, the strengths and weaknesses of each approach can be identified, providing valuable references for formulating national regulatory policies.

2.1 The EU's Emphasis on Data Protection and Privacy

The European Union (EU) has a complex regulatory framework for smart contract applications, covering areas such as financial technology, data protection, and contract

law. Overall, the EU sets a high priority on data protection and privacy, focusing on protecting consumer rights, maintaining market order, and mitigating financial risks. The EU's regulatory strategy aims to promote technological innovation while ensuring legal certainty and fair market competition. Therefore, the EU primarily relies on existing legal frameworks for smart contract regulation, such as the General Data Protection Regulation (GDPR), the Electronic Identification, Authentication and Trust Services Regulation (eIDAS), and the Anti-Money Laundering Directive (AMLD).[4]

These existing legal institutions provide a foundation for the EU's regulation for smart contract applications. For instance, GDPR establishes basic principles for data processing, including legality, minimization, accuracy, and storage limitation. Smart contract applications must adhere to these principles when handling personal data to protect users' privacy rights. In the financial sector, particularly in transactions involving cryptocurrencies, smart contract applications must comply with the EU's anti-money laundering and counter-terrorism financing regulations, which include transaction monitoring, customer identity verification, and reporting of suspicious transactions. Additionally, eIDAS provides legal recognition for electronic signatures and identities, which is crucial for the legal validity of smart contracts. Smart contracts can be regarded as electronic contracts, and their signatures and execution must comply with eIDAS requirements.

2.2 The US's Encouraging Attitude Towards Digital Assets

The United States has demonstrated a proactive and forward-looking attitude when it comes to the regulation of smart contracts and blockchain technology. Since 2018, the U.S. has been introducing a series of policies related to digital assets, especially cryptocurrencies and Non-Fungible Tokens (NFTs). [5] These policies aim to balance security and innovation while enhancing the foreseeability of the regulatory system.. For example, in the case *Rensel v. Centra Tech, Inc.*, the U.S. District Court for the Southern District of Florida made a landmark ruling on smart contract enforceability.[6] Without evidence to prove otherwise, the smart contract defined the parties' rights and obligations, showing it had legal enforceability. Second, the U.S. is committed to implementing policies to ensure the rational and healthy development of its blockchain industry. The U.S. has issued policy guidelines to encourage the industry to view blockchain technology objectively and rationally, recognizing its positive value while avoiding unconsidered investments and applications. Third, the U.S. actively works to prevent security risks associated with blockchain technology. The U.S. strengthened oversight of criminal activities involving digital currencies, launching the "Digital Currency Cleanup Operation" to predict and mitigate risks through preventive measures.[7] Furthermore, the federal government allows states to formulate their own policies and regulations to accommodate different applications of blockchain technology. For example, Illinois enacted the Blockchain Technology Act, which permits the use of blockchain in commercial activities and prohibits local governments from restricting blockchain or smart contracts.

2.3 Japan's Focus on Digital Transactions

Japan has established a comprehensive regulatory framework for blockchain and cryptocurrency, positioning itself as a global leader in Web 3 innovation. The country legally recognized cryptocurrencies as a payment method through the amendment to the Payment Services Act (PSA). Japan's recent reforms include allowing venture capital investments in Web 3 startups, and streamlining token listing processes. Starting in 2018, Japan began gradually improving its regulatory framework by issuing guidelines and regulations to standardize the issuance and trading of digital currencies. Although many regulatory rules are still in their early stages, the Japanese government is promoting the healthy development of digital transactions through progressive compliance measures. For example, Japan requires trading institutions to register and continuously strengthens measures for fund segregation and anti-money laundering. These measures, while strictly regulating digital currencies, also provide support for the widespread application of blockchain technology.

2.4 South Korea's Focus on Investor Rights Protection

South Korea's regulatory framework for smart contracts and virtual assets is gradually improving, aiming to protect investor rights, promote healthy market development, and align with international regulatory trends. The South Korean government has been highly active in legislating for cryptocurrencies and blockchain. In 2023, South Korea passed the Virtual Asset User Protection Act, aimed at protecting investors and establishing a healthy market order. The new act emphasizes the protection of investor rights, requiring virtual asset service providers (VASPs) to facilitate cold wallet technologies and establish cybersecurity incident reserves. The act also regulates unfair trading practices such as insider trading and market manipulation, requiring operators to establish systems for monitoring and reporting. Furthermore, South Korea adopts a zero-tolerance policy toward unfair trading practices, including the use of undisclosed material information, market price manipulation, and fraudulent trading activities. Violators face criminal and administrative penalties, including imprisonment and fines. Additionally, the Financial Services Commission (FSC) and the Financial Supervisory Service (FSS) play significant roles in South Korea's virtual asset regulation. The FSC oversees and regulates the cryptocurrency industry, while the FSS handles specific enforcement and supervision tasks.[8]

2.5 The UK's Innovation in "Regulatory Sandbox"

Additionally, the United Kingdom's "regulatory sandbox" mechanism for smart contract applications is particularly noteworthy. The regulatory sandbox, established by the Financial Conduct Authority (FCA) to address the rapid development of financial technology, provides a controlled environment for fintech companies to test innovative products, services, and business models in real market conditions while ensuring consumer protection and financial market stability. The core feature of the regulatory sandbox is that it provides a "safe space" where companies can temporarily operate free

from conventional regulatory constraints and conduct periodic testing of their products and services. Participating companies must apply and, upon FCA approval, receive sandbox tools and dedicated support to facilitate their testing. The sandbox not only reduces the time and cost of bringing innovative projects from concept to market but also mitigates regulatory uncertainty, facilitating corporate financing. Through the regulatory sandbox, the FCA collaborates closely with innovative companies to ensure that new products and services protect consumer interests while promoting the application of blockchain technology. However, despite its significant success in fostering innovation, the regulatory sandbox faces challenges such as limited business types and scale, which may impact the exposure of large-scale risks and the demonstration of business advantages.

3 Status and Challenges: China’s Regulation of Smart Contract Application

While the Chinese government has adopted a strict regulatory approach towards the circulation of bitcoin and other cryptocurrencies, China has affirmed the development of blockchain technology and its application by leading tech companies. The Blockchain Information Service Management Regulations, implemented on February 15, 2019, and the first batch of registered entities announced on March 30, reflect the need for standardized regulation while clarifying the scope of industry applications through a registration system. This aims to reduce illegal activities involving blockchain and promote the industry’s development toward legality and compliance. The government particularly emphasizes the potential of blockchain technology in areas such as finance, public services, and government affairs, and has outlined several key areas for breakthroughs in smart contract applications.[9] Notably, in state-led applications such as government data, digital courts, and digital government initiatives, smart contracts have become a critical foundational technology.

While smart contracts have been applied in certain areas, achieving broader-scale effects requires further efforts in technological innovation, regulatory development, and market cultivation. The lack of detailed regulatory rules for specific industries and the potential for deceptive practices pose significant challenges.. Over the past decade, the number of judicial cases related to smart contracts in China has shown a growing trend (see Figure 1).

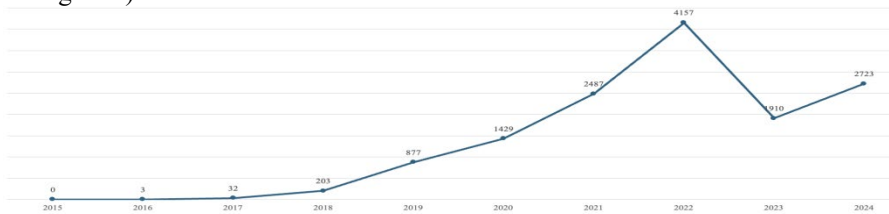


Fig. 1. Judicial cases related to smart contracts in China over the past decade

In light of this, for the compliant supervision of smart contract applications, first and foremost, it is essential to adhere to the fundamental principle of balancing supervision and innovation, striking a balance between innovation and supervision to avoid falling into the dilemma of "stifling innovation with excessive regulation and causing chaos with lax regulation." On the one hand, in China, smart contract technology has given rise to a series of innovative scenario-based applications, such as digital collectibles and smart contracts for the digital yuan. The new solutions provided by smart contracts are of great significance in empowering the development of the digital economy. Therefore, regulatory authorities should avoid stifling the innovation related to smart contract applications due to excessive regulation. On the other hand, legal supervision of smart contracts is obviously necessary. Ensuring the legality and compliance of smart contract applications and preventing the occurrence of illegal and immoral behaviors are of great significance for protecting the legitimate rights and interests of individuals and maintaining the overall market order.

4 Pathway Forward: Smart Contract Regulation Based on Virtual Communities

4.1 Limitations of Existing Regulatory Approaches

China's regulatory landscape for smart contracts faces dual challenges: fostering innovation in state-led applications while addressing risks in market-driven scenarios, evidenced by the rising volume of judicial cases spanning civil disputes to criminal activities. The comparative analysis in Section 2 reveals that existing international frameworks, despite their merits, exhibit structural limitations that hinder their adaptability to China. The US model suffers from fragmentation due to divergent state-level policies, increasing compliance costs for cross-state operations. Similarly, the EU's reliance on laws such as GDPR and eIDAS creates coordination challenges, as ambiguous jurisdictional boundaries between overlapping regulations complicate compliance for smart contract applications. Japan and Korea's approach lacks mechanisms to address emergent technical risks due to their reactive regulatory posture. Regarding the UK's regulatory sandbox, although it is an effective regulatory technique, it does not function as an overarching regulatory framework for the large and diverse smart contract ecosystem in China.

These shortcomings underscore the need for a hybrid regulatory paradigm that transcends unilateral approaches. Specifically, China's pathway must reconcile two imperatives: (1) preserving the autonomy of smart contract ecosystems through community self-governance, and (2) embedding legal safeguards within technical architectures to mitigate the potential risks to the society.

4.2 Community Self-Governance and Indirect Regulation

In the face of these challenges, community self-governance can be leveraged to alleviate them. Firstly, encourage the resolution of disputes within the community. By

formulating user service agreements and community conventions, trading habits can be formed, and the automated regulation of the dispute resolution mechanism through code can reduce the reliance on external legal intervention.[10] Secondly, define the boundaries of legal intervention. Taking community self-governance as the main principle, the law should only intervene as a supplement when disputes cannot be resolved within the community or when public interests are damaged, so as to avoid hindering community innovation. Thirdly, promote the coordinated evolvement of technology and law. Establish a flexible legal framework that allows communities to embed governance rules into the technical architecture while carrying out sandbox supervision at the same time.[11] Fourthly, promote industry self-discipline and evaluation systems. Formulate self-discipline guidelines and build a full-process evaluation system to reduce regulatory arbitrage.

For the compliance regulation of smart contract applications, the fundamental principle is to balance regulation and innovation, avoiding the dilemma of “overregulation stifling innovation” or “underregulation leading to chaos.” On one hand, smart contract technology has already enabled a series of innovative applications, empowering the development of the digital economy. Therefore, regulatory authorities should avoid stifling innovations through excessive regulation. On the other hand, legal regulation of smart contracts is clearly necessary. Ensuring the legality and compliance of smart contract applications is of utmost importance. It serves to prevent illegal or unethical behavior and safeguards individual rights as well as the overall market order.

Based on the above principle, the specific implementation pathway for compliance regulation should follow a strategy of indirect regulation by utilizing the self-governance of virtual communities. Virtual communities are digital relational networks that enter the legal domain via contractual relationships. Platform user agreements, a major part of community norms, are legally recognized as contracts. These contractual relationships serve as a key means for legal analysis of social relationships. Through the smart contract virtual community framework, the legal dimension of social groups behind contracts becomes clear.

For the diverse and innovative development of smart contract applications, internal self-governance within virtual communities plays a significant role. It is beneficial in terms of value diversity, contractual freedom, and at the same time, helps in reducing institutional costs and encourages digital economy innovation. First, community self-governance facilitates value diversity and mechanism innovation within smart contract virtual communities. Virtual communities, with their flexible structures and norms, provide fertile ground for exploring new forms of property. For example, in the field of smart contracts, automated execution functions can enable “dividends” or “taxation” during the transfer of smart contracts, implementing a certain distribution mechanism for profits within the community. Such profit distribution mechanisms are typically stored as program code in blockchain protocols, thereby creating binding constraints on all members of the smart contract virtual community through the technical architecture.

As is displayed in Figure 2, the concept of virtual community self-governance can be explained through the following four layers. At the bottom layer, fundamental technologies like cryptography, consensus mechanisms, blockchain, and contract language

form the groundwork. Then it comes to the architecture layer and the norms layer of virtual communities. Each community has its technical architecture (e.g., ETH, Ripple, etc.) and community norms such as user agreements and community contracts. On top is the application scenario layer, which might vary from case to case, covering applications such as cryptocurrencies, digital collectibles, supply chain finance, and so forth.

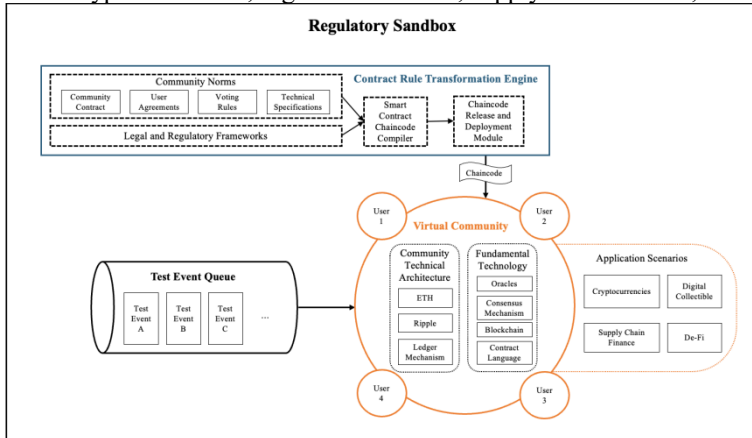


Fig. 2. Regulation Based on Virtual Community Self-Governance

It is crucial to note that community self-governance does not mean a lack of regulation; rather, it is a form of indirect regulation. The community still operates within the boundaries of the law. The social interaction patterns in smart contract virtual communities depend on community norms established by agreements, conventions, or rules, which form legally binding contracts. This indicates that the community norms, agreements, and rules must be constrained by public interest and public order, including the financial system's stability, the protection of consumers' legitimate rights, and the prevention of illegal activities.

5 Evaluation Metrics for Smart Contract Application Regulation and Compliance

Conducting regulatory evaluations for smart contracts is the foundation for the overall regulatory mechanism. Therefore, a comprehensive evaluation metrics system is necessary for the regulation of smart contract applications.

The metrics system incorporates both self-regulation and external regulation characteristics. The orderly development of smart contract applications ultimately relies on a well-functioning overall order within the smart contract community, supplemented by robust legal and regulatory frameworks as a safety net to promote diverse innovation in smart contracts.[12] Therefore, the regulation of smart contract applications cannot be simplified into a compliance issue for a single entity. Guided by this principle, our regulatory evaluation system integrates multiple evaluation methods, including questionnaire scoring, expert scoring, and model scoring, as well as multiple implementing

entities such as platforms, regulatory authorities, and third-party auditors. This would facilitate the collaboration between different entities. Through flexible arrangements in evaluation methods, implementing entities, and regulatory approaches, the proposed Smart Contract Regulatory Evaluation Metrics System maximizes the balance between innovation and regulation. This helps establish a smart contract regulatory framework based on community self-governance, supplemented by legal and regulatory measures, effectively enhancing regulatory capacity and efficiency.

5.1 The Three-Stage Design of Metrics Indicators

Based on an analysis of the characteristics of a full-chain compliance regulatory system for smart contracts, a smart contract regulatory capability metrics system is proposed, creating a full-chain compliance regulatory framework covering the ex-ante, interim, and ex-post stages. This ensures technological innovation in smart contracts while enhancing regulatory capacity and efficiency.

In the ex-ante review stage, the metrics system focuses on evaluating multiple aspects of the smart contract applications, including code accuracy, clarity of terms, authenticity of intent, risks of code centralization, compliance with community norms, and legality of contract content. This ex-ante review stage stops vulnerable smart contract applications from going into the market from the beginning.

During the interim behavior monitoring stage, the regulation focus is on the runtime execution of smart contract applications. Since there is a gap between the build-time/compile logic and the runtime execution in runtime, this stage is of special importance in order to monitor the system behavior, identify errors and risks, and prevent the potential harm to the users. Regulation technologies such as multi-signature and privacy-preserving computation could be leveraged to enhance transparency and consistency while ensuring the legitimate rights of relevant parties.

In the ex-post management and auditing stage, the focus is on handling contract disputes, post-audit, and user privacy protection. By establishing mechanisms like smart arbitration for dispute resolution, disputes arising during contract execution can be resolved quickly and effectively. Additionally, via data mining techniques, the operational status of smart contract systems can be deeply analyzed so as to identify abnormal behavior and potential risks.

5.2 Key Indicators in the Regulation Evaluation Metrics System

Formulated under the principle of balancing innovation and regulation, the metrics system aims to develop legal regulatory recommendations that both promote innovation and ensure compliance. As shown in Table 1, the metrics system establishes 11 secondary indicators and 46 tertiary indicators, covering ex-ante review, interim monitoring, and ex-post auditing.

Table 1. Smart Contract Application Regulation Evaluation Metrics

Stage	Metrics		Level	Evaluation		
I Ex Ante	I-1 Accuracy Review	I-1-1 Accuracy of Contract Code	Excellence	Q	P	S
		I-1-2 Clarity of Contractual Terms	Compliance	Q	P	S
		I-1-3 Authenticity of Intent Expression	Compliance	Q	P	S
		I-1-4 Witnessing of Intent Expression	Compliance	Q	P	S
		I-1-5 Anti-Fraud Mechanisms	Compliance	E	G	R
	I-2 Security Review	I-2-1 Code Auditability	Compliance	E	T	S
		I-2-2 Code Security	Compliance	E	T	S
		I-2-3 Code Centralization Risk	Compliance	E	T	S
		I-2-4 Identity Verification	Compliance	Q	P	S
		I-2-5 User Information Security	Compliance	E	T	R
	I-3 Consistency Review	I-3-1 Contract Mapping Integrity	Excellence	M	P	S
		I-3-2 Consistency Test Mechanism	Excellence	M	P	S
	I-4 Regulatory Compliance Review	I-4-1 Recordation Registration	Compliance	E	G	R
		I-4-2 Community Norm Compliance	Excellence	Q	P	S
		I-4-3 Legality of Contract Terms	Compliance	Q	G	R
		I-4-4 Organizational Decision-Making	Compliance	Q	G	R
		I-4-5 Technical standards compliance	Compliance	Q	G	R
	I-5 Platform Reliability Review	I-5-1 Clarity of Subject of Responsibility	Compliance	Q	G	R
		I-5-2 Timestamp Reliability	Compliance	Q	P	S
		I-5-3 Oracles Reliability	Compliance	Q	P	S
		I-5-4 Reliability of Network Interactions	Compliance	Q	P	S
		I-5-5 Key Reliability	Compliance	Q	P	S
	I-6 Regulatory Sandbox and Risk Level	I-6-1 Risk Level System	Excellence	Q	G	R
		I-6-2 Regulatory Sandbox	Excellence	Q	G	R
		I-6-3 Label Management	Excellence	Q	G	R
II Interim	II-1 Contract Modification Monitoring	II-1-1 Multi-Signature Consent	Compliance	Q	P	S
		II-1-2 Regulatory Reporting	Excellence	Q	P	S
		II-1-3 Right to Know Protection	Compliance	Q	P	S
	II-2 Contract Execution Monitoring	II-2-1 Real-Time Execution Monitoring	Excellence	Q	P	S
		II-2-2 Execution Process Compliance	Excellence	E	T	S
		II-2-3 Execution Deviations Preventing	Excellence	Q	P	S
		II-2-4 Execution Risk Management	Excellence	Q	P	S
		II-2-5 Monitoring Test Coverage	Excellence	Q	P	S
		II-2-6 Stakeholder Protection	Compliance	Q	P	S
	II-3 Contract Termination Review	II-3-1 Termination Conditions Review	Excellence	Q	P	S
		II-3-2 Termination Notification	Excellence	Q	P	S
		II-3-3 Termination Information Archiving	Excellence	Q	P	S
III Ex Post	III-1 Contract Dispute Resolution	III-1-1 Dispute Resolution System	Excellence	Q	P	S
		III-1-2 Multiplicity of Dispute Resolution	Excellence	Q	P	S
		III-1-3 Dispute Evidence Preservation	Compliance	Q	P	S
		III-1-4 Remedy Implementability	Excellence	Q	P	S
		III-1-5 Integration of Dispute Resolution Systems	Excellence	Q	P	S

Stage	Metrics		Level	Evaluation		
III-2 Ex Post Audit	III-2-1	Log Mining Analysis	Compliance	Q	P	S
	III-2-2	Community Ledger Integrity	Compliance	Q	P	S
	III-2-3	Remedies for User Privacy	Excellence	Q	P	S
	III-2-4	Liquidation Disclosure	Excellence	Q	P	S

The Evaluation column encompasses three key dimensions: evaluation methods, evaluation entities, and underlying regulatory philosophies. Evaluation methods include questionnaire scoring (Q), which gathers structured responses and quantifies them into scores; expert scoring (E), where domain specialists assess smart contracts based on their expertise; and model scoring (M), which relies on predefined analytical frameworks for objective assessment. Evaluation entities consist of platforms (P), which assess smart contracts from an operational standpoint; governmental authorities (G), ensuring legal and regulatory compliance; and third-party entities (T), providing independent evaluations. The underlying regulatory philosophies are self-governance (S), where virtual communities establish and enforce their own rules, and direct regulation (R), in which external bodies impose regulatory oversight.

This multi-dimensional approach ensures that the regulation of smart contracts comprehensively addresses the main risk points across the entire process while being tailored to different regulatory aspects and application scenarios. Moreover, the metrics system categorizes indicators into compliance indicators and excellence indicators. Compliance indicators refer to the basic requirements that should be met, serving as the minimum requirements to ensure the normal operation of the full-chain smart contract regulatory system. Excellence indicators, on the other hand, aim to enhance performance, optimize user experience, or achieve excellence, which goes beyond the basic requirements for regulatory purposes. Besides, the evaluation adopts a scoring system, with the scores weighted and accumulated to obtain an overall evaluation score. It should be noted that the weights of the scores can also be dynamically adjusted to accommodate the specific regulation goals for different smart contract applications.

Through continuous improvement and adaptation, the smart contract regulatory evaluation metrics system will become a vital tool in advancing the development of the smart contract industry, providing a solid foundation for balancing innovation and compliance regulation.

6 Conclusion

In the context of China's growing digital economy, the regulation of smart contracts demands innovative solutions. Our research introduces a community self-governance and indirect regulation framework, which is pivotal in reconciling innovation and compliance. By harnessing the contractual autonomy of virtual communities, this framework promotes technological innovation while ensuring regulatory compliance, and at the same time aligns with basic civil law principles. The proposed three-stage evaluation metrics system, covering ex ante review, interim monitoring, and ex post audit, offers practical value for smart contract regulation. With 11 secondary and 46 tertiary indicators, it comprehensively addresses risks across the smart contract lifecycle. The system integrates multiple evaluation methods and entities, balancing innovation and

regulation effectively. Overall, these contributions provide a solid foundation for fostering a vibrant yet orderly ecosystem for smart contract applications, where virtual communities play a central role in driving sustainable industry development.

Acknowledgments

This work is supported by the young scientists project of national key research and development “Innovative Theory and Methods of Smart Contracts and Law” with Grant no: 2022YFB2701800.

References

1. Ferreira, A.: Regulating Smart Contracts: Legal Revolution or Simply Evolution? In: Telecommunications Policy 45(2), 102081-102090 (2021)
2. Hsiao, J.: "Smart" Contract on the Blockchain-Paradigm Shift for Contract Law? In: US-China Law Review 14(10), 685-694 (2017)
3. Mewha, H.: Blockchain Wakes: Balancing the Light and Dark Sides of Blockchain through Global Regulation. In: Colorado Technology Law Journal 22(1), 59-120 (2023)
4. Han, S., Park, S.: A Gap Between Blockchain and General Data Protection Regulation: A Systematic Review. In: IEEE Access 10, 103888-103905 (2022)
5. Brookes, A.: U.S. Regulation of Blockchain Currencies: A Policy Overview. In: American University Intellectual Property Brief 9(2), 75-105 (2018)
6. Rensel v. Centra Tech, Inc., No. 17-cv-24500 (S.D. Fla. 2019).
7. Zhao, L.: Governing the Chain by Law: Technical Applications and Legal Regulation of Blockchain. In: Legal Application, Issue 3, 33-49 (2020)
8. Lee, J.: An Introductory Review of Virtual Asset Regulations in Korea. In: Journal of Korean Law 23, 391-412 (2024)
9. Gong, Q., Ban, M., Zhang, Y.: Blockchain, Enterprise Digitization, and Supply Chain Financial Innovation. In: Management World 37(2), 22-34 (2021)
10. Filatova, N.: Smart Contracts from the Contract Law Perspective: Outlining New Regulatory Strategies. In: International Journal of Law and Information Technology 28(3), 217-242 (2020)
11. Filippi, D.P., Mannan, M., Reijers, W.: Blockchain Technology and the Rule of Code: Regulation via Governance. In: George Washington Law Review 92(6), 1229-1280 (2024)
12. Efimova, L., Sizemova, O., Chirkov, A.: Smart Contracts: Between Freedom and Strict Legal Regulation. In: Information & Communications Technology Law 30(3), 333-353 (2021)

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

