Proceedings of the 3rd International Conference on Management Research and Economic Development
DOI: 10.54254/2754-1169/178/2025.22517

Legal Analysis and Rule Construction of Smart Contracts

Bolong Yin

Faculty of Law and Justice, The University of New South Wales, Sydney, Australia
yinbolong1006@outlook.com

Abstract: In the context of the boom in blockchain technology since 2008, the range of applications for smart contracts, which were first introduced in 1995, has been expanding. Their development, however, has been hampered by legal issues. The legal research on smart contracts is of great significance. Theoretically, it challenges and enriches the traditional contract theory and legal system. From a practical point of view, it helps regulate its application and protect the rights of parties in various fields such as finance and supply chain. This article delves into the legal nature of smart contracts, analyzing their relevance to traditional contract elements such as offers and acceptance. It also discusses the protection difficulties such as the difficulty of contract modification, the difficulty of contract rescission and the difficulty of contract validity. Suggested solutions include incorporating it into the existing legal system and using soft law for regulation. In summary, although smart contracts face challenges, with the development of technology and the improvement of laws, their intelligent development prospects are broad, and will drive social innovation.

Keywords: smart contracts, legal nature, contract law, rule construction, blockchain

1. Introduction

The concept of "smart contracts" was first introduced in 1995 by cryptographer Szabo, who noted that "smart contracts facilitate the execution of contracts through the use of protocols and user interfaces" [1]. In 2008, Satoshi Nakamoto published a white paper on Bitcoin, which not only marked the birth of Bitcoin, but also opened a new era of blockchain technology. People were surprised to find out that the underlying technology of the blockchain and smart contracts naturally fit, and the automatic execution of smart contracts on the blockchain is completely feasible in theory. Since then, smart contracts have been reborn, and blockchain has gradually become the most important computing scenario for smart contracts [2]. With the continuous development and improvement of blockchain technology, the application range of smart contracts continues to expand.

The definition of smart contract is: "a computer program that is able to make decisions when certain prerequisites are met", contracts can range from very simple transactions executed within seconds or minutes to relatively complex and lengthy transactions [3]. It can be seen that the object of smart contract is a legal contract, and the computer protocol is a means to ensure contract negotiation and performance, the purpose of the means is to promote, verify and strengthen contract negotiation and performance, and the digital way is the expression of the means [4]. Smart contracts are also known as blockchain smart contracts, the carrier of which is the blockchain, which is essentially a self-executing computer code. The code describes the terms of the agreement between

DOI: 10.54254/2754-1169/178/2025.22517

the buyer and seller and is written directly into the blockchain's lines of code, which is automatically executed when predetermined terms and conditions are met [4].

The characteristics of smart contracts are as follows: The first characteristic is anonymity. To protect the privacy of a user's identity, smart contracts can be anonymized with the help of a variety of technologies. Smart contracts achieve anonymous storage and verification of user identity attributes on the public blockchain, thus solving the contradiction between the public nature of the blockchain and the protection of identity privacy to a certain extent [5].

The second characteristic is autonomous execution. Smart contracts provide protocol procedures defined by the participants themselves. Participants define the rules and regulations established by the smart contract and deploy them after mutual agreement. Once a blockchain reaches a specific predefined state, it should automate the flow of programming conditions and events [6].

Furthermore, one distinguishing characteristic of smart contracts is transparency. Transparency is one of the distinguishing features that smart contracts have inherited from blockchain. The code defined in smart contracts is transparent to both intermediaries and the public, and the set of transactions contained in the blockchain is also transparent to the public. Therefore, intermediaries in the blockchain network can trust the logic and transactions in the blockchain network [6].

As an important application of blockchain technology, the development and application of smart contracts are of great significance to promote the digital transformation of the economy and society. However, due to the limitations of science and technology at that time, smart contracts remained more in the theoretical concept stage and were not widely used. At the same time, the legal issues of smart contracts have also become an important factor restricting their development. Therefore, it is of great theoretical and practical significance to study the legal nature and protection of smart contracts. From the perspective of theoretical significance, the emergence of smart contracts challenges the traditional contract theory and legal system. Studying the legal nature and protection mechanism of smart contracts is helpful to enrich and improve the traditional contract theory and legal system, and promote the innovation and development of legal theories. The automatic execution and other characteristics of smart contracts are significantly different from traditional contracts, so it is necessary to analyze and understand the legal nature of smart contracts from a new perspective and theoretical framework. At the same time, studying the legal protection mechanism of smart contracts is also helpful to solve the legal problems faced by smart contracts in practice, and provide theoretical support for the healthy development of smart contracts. From a practical point of view, the wide application of smart contracts in finance, supply chain, medical and other fields make it urgent to study the legal nature and protection mechanism of smart contracts. Clarifying the legal status and legal effect of smart contracts and establishing a sound legal protection mechanism for smart contracts will help regulate the application and development of smart contracts, protect the legitimate rights and interests of the parties, and promote the healthy development of blockchain technology. This paper will study the legal nature and protection dilemma of smart contracts, discuss how to protect smart contracts in law, and put forward prospects for the development and application of smart contracts in the future.

2. The legal nature and protection dilemma of smart contracts

2.1. The legal nature of smart contracts

In traditional jurisprudence, a contract is an agreement between equal subjects to establish, change and terminate the relationship of civil rights and obligations, and a smart contract in a broad sense refers to a computer agreement agreed between multiple parties, which seems to be conceptually in line with a traditional contract. In the world legal system, the establishment of a traditional contract must include offer and acceptance. The laws of various countries have made relevant provisions on

DOI: 10.54254/2754-1169/178/2025.22517

offer and acceptance. For example, Article 472 of the Civil Code stipulates that an offer is an expression of intent to conclude a contract with another person, which shall meet the following conditions: (1) the content is specified; (2) indicates that by acceptance, the offeror is bound by the expression of intent [7]. Since smart contracts are composed of digital codes and automatically perform the contents of the contract, the content of the smart contract must be clear, otherwise the code will not be able to perform properly or it will be difficult to perform according to the intent of the contracting party. Therefore, the other party receiving the offer can clearly know the content of the offeror's expression of intent and choose whether to execute the code [8]. After the smart contract is started, both parties cannot stop it and are not affected by the further actions of one party to the contract, which indicates that the smart contract publisher is bound by the content of its contract. In summary, a published smart contract can be considered an offer [8].

Acceptance is an expression of the offeree's intention to agree to an offer. The content of the acceptance should be consistent with the content of the offer. If an offer has a certain duration, the acceptance must be made and reach the offeror before the expiration of that duration. There is a view that smart contracts are commitments expressed in digital form and are not fundamentally different from traditional contracts [9]. Unlike traditional contracts, the promise of a smart contract comes from fulfillment. A person initiating a smart contract can post the code to the blockchain as an offer, and once an action initiates acceptance, for example by handing over control of a certain amount of money to the code, a contract is formed. However, in the initial phase of the contract agreement, there is no significant difference between smart contracts and traditional contracts. This is because before any contractual conditions can operate, both parties must agree on some terms to initiate the procedure [8]. When the offeree completes the corresponding operation according to the manner stipulated in the contract, and the operation is successfully recorded by the blockchain network, the acceptance becomes effective. The distributed ledger nature of the blockchain gives the record immediacy and immutable credibility, and once the record is completed, it indicates that the promise has been made and is effective. For example, in a blockchain-based copyright transaction smart contract, the buyer completes the payment operation in accordance with the contract requirements, the payment information is recorded on the blockchain, at this time the commitment takes effect, and the smart contract automatically performs the copyright transfer operation.

Therefore, for smart contracts, it is issued by the parties and committed by the counterparties. A smart contract can be regarded as a legal contract because of its complete offer-to-acceptance structure.

2.2. The protection dilemma of smart contracts

However, there are some difficulties in protecting smart contracts under traditional contract law, some main reasons are as follows. The first reason why traditional contract law is difficult to regulate smart contracts is that smart contracts cannot be modified and terminated. The conclusion of a traditional contract is a process in which the two parties negotiate repeatedly on the terms of the contract through face-to-face communication, email exchanges or other means, and finally reach an agreement. During the performance of a traditional contract, if the parties reach a consensus through consultation, the contents of the contract may be modified. Smart contracts are often written by one party in advance and deployed on the blockchain, and other participants can only choose to accept or not accept, without the right to negotiate changes to the terms. Once a smart contract is deployed on a blockchain, it is difficult to undo or change it due to its immutable nature. Therefore, if the code of a smart contract has errors or needs to be adjusted to changes in the market, it is difficult to deal with it as flexibly as a traditional contract. Therefore, if the parties to the smart contract do not perform the contract, then the questions of "how the law determines whether the smart contract is terminated" and "how the law

DOI: 10.54254/2754-1169/178/2025.22517

determines the smart contract is terminated" are placed in front of the theoretical and practical circles [10].

Tracing the development of world jurisprudence, the contract formation system is the cornerstone of the contract legal system, which is used to fix the transaction agreement between the parties. And the contract validity system is gradually enriched and refined, from simply focusing on the form of the contract to taking into account the substantive fairness and transaction security. Usually, the validity of the contract comes into effect when it is formed, but when there are certain circumstances such as fraud and coercion, it will affect the validity of the contract according to the doctrine of meaning. For smart contracts in the blockchain, once the parties enter the contract, the contract will be automatically executed until the completion of the contract. Will the parties' expressions of intent differ in smart contracts? If there is an inconsistency and a negative legal assessment, what should be done with a self-executing contract [10]? These are questions worth thinking about. As a form of expression of smart contracts, computer code is significantly different from natural language. Because the opposite party of smart contracts is usually unfamiliar with computer code, it is easy to have major misunderstandings and other untrue expressions of meaning when they cannot fully understand the contents of the contract. Therefore, the effectiveness of the contract system for smart contracts executed by technical guarantees appears to be difficult at present [10].

Finally, the anonymity of smart contracts may make it difficult for a party to remedy rights under traditional contract law. For example, in the Ethereum crowdfunding project scenario, if fraudulent situations such as false projects occur, investors participating in the crowdfunding may suffer losses. At this time, the validity of the smart contract needs to be judged by the court, but the anonymity of the blockchain makes it very difficult to determine the initiator of the crowdfunding project, and it is difficult to meet the requirement of "there is a clear defendant" in the filing conditions, resulting in the judicial process is difficult to start. In addition, even if the smart contract is found to be invalid or can be changed or revoked, for the smart contract that has been completed, according to the contract law, the project sponsor shall return the property obtained by the contract. However, in practice, due to the difficulty in identifying the responsible person, the realization of these property return, discount compensation or compensation for the loss of measures will face difficulties [10].

3. Rules building for smart contracts

Incorporating smart contracts into the existing legal system is a viable legislative model. This model can make full use of the existing legal framework and system, reduce the cost of legislation, and improve the stability and predictability of law. From the perspective of contract law, smart contracts meet the basic characteristics of contracts to a certain extent, such as the agreement between the parties, the agreement of rights and obligations, etc., and can be included in the adjustment scope of contract law. However, as mentioned earlier, there are certain difficulties in regulating smart contracts in traditional contract law. This requires improving the relevant contract system, reasonably defining the establishment and execution of smart contracts at the technical level, so that they are in line with the contract law system. Technology users need to work with legal experts to create accurate contract code rules to reduce legal risks and improve the formation rules of smart contracts [11]. Through the interpretation and amendment of the contract law, it can clarify the nature of the contract, the way of conclusion, and the validity of the smart contract, so that it can apply the relevant provisions of the contract law. For example, in traditional contract law, special clauses on smart contracts can be added to regulate the special problems of smart contracts.

When incorporating smart contracts into traditional legal systems, it is essential to adhere to core private law principles. It is necessary to adhere to and realize the application of private law principles in modern technology smart contracts as much as possible, rather than allowing the development of technology to be unregulated. Smart contract technology limits the role of the traditional complex

DOI: 10.54254/2754-1169/178/2025.22517

expression of will system, has a great impact on the withdrawal of offer, revocation and withdrawal of acceptance, and endangers the autonomy of the parties' will and freedom of choice advocated by the contract system. However, it should be emphasized that when the smart contract is generated, the negotiation on the contract is reached by fully respecting the expression of the intention of the experts and the contractor, and technically through the contract verification on the virtual machine, to ensure the consistency of the code and the contract text of the contract execution process [12]. In addition, the biggest contribution of smart contracts is to build a sound trust mechanism through technical means, but this does not mean that the traditional principle of honesty and credit is abolished. Although the rigidity of the machine causes the principle of good faith to temporarily lose the operating space of the traditional principle of good faith, with the development of technology at the cognitive level and the humanization and flexibility of the underlying protocol design, the role of the principle of good faith may be revealed again [12].

In addition, smart contracts are very advanced from a technical point of view and play a key role in the security of the blockchain and the security of transaction information [10]. Each block in the blockchain contains specific information, and the unidirectional nature of hash function operations makes reverse operations almost impossible, thus guaranteeing the security of transaction information. At the same time, the consensus mechanism among strangers ensures that honest nodes make real transaction records from a probabilistic and statistical sense [10]. Smart contracts explicitly "if... then…" The mechanism is designed to ensure that transactions are automatically executed. These mechanisms around security, credibility, and automatic execution are all arrangements that take various factors into account in advance, which are preventive measures, and there is no post-relief system design such as liability for breach of contract and damage compensation in the entire smart contract design architecture [10].

Therefore, in the scope of smart contract regulation, "replace hard law with soft law, and turn post-relief into pre-prevention" is a reasonable and necessary strategy [13]. Some scholars have proposed embedding a third-party trigger mechanism in smart contracts, however, this may not only face technical and cost difficulties, but more importantly, run counter to the spirit of blockchain democracy. In the "two decentralized and two centralized" structure of smart contracts, the consensus mechanism plays the role of "regulator", and elements such as compilation logic ensure that smart contracts reach consensus and operate smoothly [13]. In this case, the soft law form of standard can effectively replace the hard law of private law to regulate smart contracts. The government should avoid direct intervention in the formulation of standards, form consensus in the industry with the help of market-oriented screening, and follow the principles of autonomy and openness [13]. Soft law focuses on pre-prevention, which can effectively filter the potential defects of smart contracts and reduce the cost of post-relief. At the same time, soft law does not attach value judgment and national will, has global universality, has more advantages in solving jurisdictional and applicable law issues, and can better adapt to the regulatory needs of smart contracts [13].

4. Conclusion

As the core component of blockchain, smart contract has broad application prospects and important development significance. At present, it has shown advantages in the field of Internet finance, such as equity crowdfunding, P2P online lending, etc., as well as asset leasing management, which can realize decentralized automatic execution and effectively solve the pain points in the traditional model. Smart contracts have the characteristics of autonomy, self-sufficiency and decentralization, and give programmable mechanisms to blockchain data, which is the basis for building programmable financial and social systems, and also helps the application of blockchain in distributed artificial intelligence systems to promote the development of decentralized applications, organizations, companies and even society. At present, blockchain and smart contract technology is evolving from

DOI: 10.54254/2754-1169/178/2025.22517

automation to intelligence, and the existing smart contracts are mostly based on "IF-THEN" conditional response rules to meet the needs of automated transactions and data processing. Future smart contracts should have "WHAT-IF" inference, computational experiments and autonomous decision-making functions to achieve a leap from "automation" to truly "intelligent", which will further expand its application in more complex scenarios and bring innovative changes to all areas of society [14].

As an important application of blockchain technology, smart contracts have great theoretical and practical value. Its appearance challenges the traditional contract theory and legal system, and enriches and innovates the legal theory. In practice, smart contracts have broad application prospects in many fields, promoting the digital transformation of the economy and society.

However, smart contracts face a number of protection dilemmas. Their difficulty in easily modifying and terminating, the nature of computer code that leads to potential problems with the effectiveness of the contract system, and the difficulty in holding unlawful use accountable under traditional contract law all hinder the development of smart contracts. To address these issues, incorporating smart contracts into the existing legal system is a viable solution. This requires improving the relevant contract system, clarifying legal provisions, and adhering to the core private law principles. In addition, adopting the strategy of "replacing hard law with soft law and turning after-the-fact relief into pre-event prevention" can better regulate smart contracts.

Moreover, when there is non-performance, whether the smart contract can continue to execute and whether external decision intervention can become a technical problem, which requires the corresponding external intervention program to be embedded in the design of computer code. In order to solve these problems, technology iteration and upgrading are imperative. At present, the application scenario of smart contracts focuses on simple contract types and virtual environments. In the future, if it is expanded to more complex and diversified contract types, it not only requires a more perfect underlying protocol of the blockchain, but also needs to use artificial intelligence cognitive technology. The deep integration of the two is an inevitable trend of future development [12].

Looking ahead, smart contracts are evolving from automation to intelligence. Although it currently faces technical challenges such as lack of suspension mechanism and limited application scenarios, with the iteration of technology and the deep integration of blockchain and artificial intelligence cognitive technology, smart contracts are expected to achieve functional leaps, expand applications in more complex scenarios, and bring innovative changes to society. In general, continuous exploration and improvement in both legal and technical aspects is crucial to the healthy development of smart contracts.

References

[1] *He.H., Yan.A.,Chen Z. (2018). Overview of smart contract technology and application based on blockchain. Computer Research and Development, 55 (11), 2452-2466.*

[2] *Liwei.O., Shuai.W., Yong.Y., Xiaochun.Ni., Feiyue.W. (2019). Smart Contracts: Architecture and Progress. Journal of Automation, 45 (3), 445-457.*

[3] *Kolvart, M., Poola, M., Rull, A. (2016). Smart contracts. The Future of Law and etechnologies, 133-147.*

[4] *Zhu Yan, Wang Jing, Guo Qian, & Liu Guowei. (2020). Research progress of blockchain-based smart contract technology. Cyberspace Security, 11 (9), 19-24.*

[5] *Borse, Y., Chawathe, A., Patole, D., Ahirao, P. (2019, February). Anonymity: A secure identity management using smart contracts. In Proceedings of international conference on sustainable computing in science, technology and management (SUSCOM), Amity University Rajasthan, Jaipur-India.*

[6] *Hewa, T. M., Hu, Y., Liyanage, M., Kanhare, S. S.,Ylianttila, M. (2021). Survey on blockchain-based smart contracts: Technical aspects and future research. IEEE Access, 9, 87643-87662.*

[7] *National People's Congress of the People's Republic of China (2020). Civil Code of the People's Republic of China, article 472.*

[8] *Jidong.C. (2019). Legal Construction of Smart Contracts. Oriental Law, 3, 18-29.*

DOI: 10.54254/2754-1169/178/2025.22517

[9] LuJie D. (2023). Research on the current status of blockchain smart contracts. Dispute Settlement, 9, 2603.

[10] Xichen.L. (2020). Blockchain smart contracts challenge traditional contract law and their responses. Journal of Xihua University (Philosophy and Social Sciences Edition), 39 (3), 94-100.

[11] Zhenguo C. (2019). Thoughts on Contract Law of Smart Contracts under Blockchain. Social Sciences in Guangdong, 4, 236-246.

[12] Yibo C. (2019). Research on the Fit between Smart Contracts and the Private Law System. Oriental Law, 2, 68-81.

[13] Wang, & Huixu.Y. (2019). Private law challenges and responses to smart contracts. Yunnan Social Sciences, 4, 127-133.

[14] Yong.Y.,Feiyue.Wang. (2016). Development status and prospects of blockchain technology. Acta Automatica Sinica, 42(4), 481-494.