Smart Contract in Blockchain

Tian Mao[1](✉) and Junhua Chen[2]

[1] Department of Law, China Jiliang University, Hangzhou, China
maotian.2@qq.com
[2] China National Institute of Standardization, Beijing, China
chenjunh@cnis.ac.cn

Abstract. Smart contract is presented as a new infrastructure for programming, deployment and execution with the rapid pace of blockchain technology in recent years. The development of blockchain technology provides a good operational basis for smart contracts, which can play an important role on the blockchain. With the rapid development of blockchain platforms such as bitcoin, smart contracts have a good opportunity for development. However, smart contract applications are still at an early stage of development, with relatively little relevant research, and the applicable scenarios of smart contracts in practical applications are not rich enough. In the paper, we study and discuss several aspects, by changing decentralization to weak-centralization, retaining appropriate supervision, and providing necessary right remedy for users of non-performance clause, can make smart contracts safe to use by compromising part of transaction efficiency.

Keywords: Smart Contracts · Weak-centralization · Standardization · Blockchain

1 Introduction

Smart contracts are a new architecture for program design, deployment and operation developed in recent years with the rise of blockchain technology.

Smart contract technology has successfully solved the problem of difficult blockchain application development by supporting more powerful programming languages and runtime environments and allowing developers to develop arbitrary value exchange-related applications on it [10], representing the future direction of blockchain technology development. However, smart contracts have limitations on autonomy and potential infringement on the property rights of the parties, which require a suitable interpretation path and regulation method in the existing legal system. In this paper, we try to find a solution to the problem of "smart contract clauses". Based on the standardization of smart contract terms and conditions, we will find a solution to the problem.

2 Implementation of Smart Contract

Smart contracts are a new stage of contract development. As shown in Fig. 1, in terms of external carriers, contracts can be classified as paper contracts, electronic contracts or

D. Qiu et al. (Eds.): ICBBEM 2022, AHIS 5, pp. 868–875, 2023.
https://doi.org/10.2991/978-94-6463-030-5_86

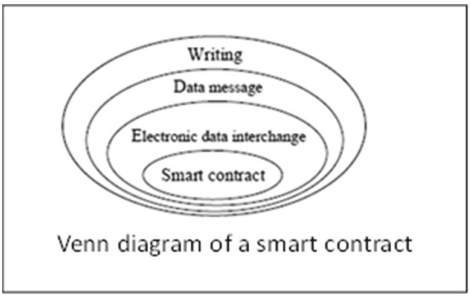

Fig. 1. Venn diagram of a smart contract

digital contracts [9]. Paper contracts are the paradigm of the former information technology era, while electronic contracts are the product of information technology. In addition to the difference in form, there is no substantive difference between the two. However, with the development of information technology and computer technology, electronic contracts have been surpassed and "data-oriented contracts" and "computable contracts" have been created. In a data-oriented contract, "the parties express the terms or conditions of their agreement in a predetermined manner that can be processed by a computer system". The primary reader is a machine, not a human. Computable contracts enable computer systems to give data-oriented contracts a capability to perform automatic, preliminary contract compliance or performance assessments [6]. There is a trend toward machine autonomy, with machines gradually replacing humans in contract negotiation, conclusion, performance, and enforcement. Smart contracts are more advanced versions that can be performed and enforced automatically without human intervention as soon as a given state is reached or a predetermined event occurs, while the above-mentioned contract types still have room for human interpretation and interference, especially for property rights transfer and value transmission dependent on one party.

Smart contracts are still based on other contracts: such as paper contracts, electronic contracts, which can be read and understood by the parties; such as data-oriented contracts, computable contracts, which can be read and executed by computer systems. Therefore, its architecture takes into account both humans and machines, and constructs a two-layer structure in the contract fundamentals: a contract text layer suitable for humans and a contract code layer suitable for machines. The text of the contract is presented in natural human language, and can be divided into plain text, which only contains the main terms or rules of the contract, and full text, which can be loaded if a full understanding of the contract is needed [2]. The contract code is written in a computer language, which is different from a computer program, but is "a mode of communication between computer programs, often described as methods, data structures, and algorithms that allow parties to exchange information precisely and efficiently". The contract code is the data base of a smart contract, which records the contract terms or rules and can be read and executed by a computer system, and the smart contract is expressed in the code and stored in the block data structure. In terms of contract text and contract code, there are correspondence, complementary and independent relationships between the two. By correspondence, the contract text reflects the description of the contract code and its

meaning; by complementarity, the contract text does not directly describe the meaning of the code, but focuses on explaining the rules of operation of the code to the user or explaining what the code does not provide; by independence, it mainly means that there is no text, but only the contract code expresses the rules of behaviour and the relationship between the parties. Many contract terms can be written in a machine-interactive programming language, but the conversion of natural language into machine-readable code limits the range of subjects and activities that can be easily and precisely defined, and there are still many terms or contract contents that cannot be described in machine language [7].

In this paper, we use the SPESC language as an example to embed legal clauses into the contract text in order to pair smart and legal contracts. The SPESC language is a transitional language between the real legal contracts and the existing general language for smart contracts [3]. Smart contracts are not limited to a specific smart contract programming language and implementation environment, and can support translation into any existing smart contract language program code and run on the platform.

In the example of a commodity purchase and sale contract, the defined terms regulate the following behaviour.

- First, the seller creates the contract and mails it by calling the post() action after the buyer places the order.
- The buyer transfers funds to the contract as payment for the goods by calling the pay() action.
- When the buyer calls receive( ) action to indicate that the goods have been received, the seller can only call collect to obtain the aforementioned funds.

```
Contract purchase(
    Party seller address
    (ID){
        Post()
        Collect()
    }
    Party Buyer{
        Pay()
        Receive()
    }
```

【Definition of parties】

```
Asset Printer: address
(ID){
  Name “printer”
  Value: 1000$
The}
```

【Definition of Asset】

Contract participants will be defined one by one, with each participant defined by a party structure, which consists of a name as an identifier, some party attributes and actions.

Each action defined in a contract participant represents an action that the contracting party can or must perform [1]. Each action is declared in parentheses, e.g., post() represents the seller's shipping action, pay() represents the buyer's payment action, etc. These actions can be implemented in multiple ways in a real contract and need not be further specified in the contract if they are already acceptable to the contract participants. Definition shows three relatively simple examples of contract participants: Seller, Buyer. The seller can perform two actions: abandon and collect; the buyer has two actions: pay and receive.

The above template is a typical example of an automatic performance clause. Although the carrier of the automatic performance clause is the code and algorithm, it manifests the parties' agreement to perform the transaction automatically. In other words, although the parties cannot understand the meaning of the program code, they expect to achieve the contractual purpose through the automatic performance feature of the smart contract.

But this can create new problems, such as not only code defects and loopholes in the technology itself, but also the problem of technical personnel understanding or writing errors when writing smart contracts, and in these cases, the parties' rights can be unreasonably restricted.

term no1: Buyer **can** pay
    While deposit $ Printer::**value**
term no2: Seller **shall** post
    When within 7 days **after** Buyer **did** pay
term no3: Buyer **shall** receive
    When within 7 days **after** Seller **did** post
term no4: Seller **can** collect
    When after Buyer **did** receive
    While withdraw $ Printer:: **value**

【Definition of contract terms】

3 Development Status and Challenges

As the popularity and application of blockchain technology continues to grow, the emerging smart contract technology has attracted widespread attention in academia and industry. Smart contracts are decentralized, de-trusted, autonomous and self-sufficient, and tamper-evident, allowing contract parties to complete transactions without any trust base or third-party trusted authority, while their embeddable digital form is expected to enable all kinds of programmable smart assets, systems and societies, deeply transforming many traditional fields such as finance, management, healthcare, and the Internet of Things [4].

term no1: Seller **can** abort
When before buyer **did** confirm Purchase
While withdraw $ XXX Description::price*2
term no2: voters **can** delegate
when voting is true and his::voted **is false**
where his::voted **is true**
term no3: Buyer **shall** receive
When after chairperson **did** Start Bidding **and before** Bidding stop time
While
deposit $ value > highest price
transfer $ highest price to highest Bidder
when highest Price = **value and** highest Bidder = this bidders

【Other applications: auction under smart contract】

The main risks are: first, the existing system is flawed in using smart contracts, and only contracts are not applicable to any scenario. Second, smart contracts rely on blockchain technology to establish, from establishment to fulfillment are inseparable from the code and algorithm, inevitably there are technical problems. The technology itself not only has code defects and loopholes, but the writing of smart contracts also has the problem of technical personnel understanding or writing errors; thirdly, there are derivative risks [5]. Due to the inherent characteristics of blockchain technology, the code on the blockchain needs to be real and valid, and the information is visualized in the form of code on the blockchain, which can be translated into common language, and the information security is difficult to guarantee.

4 Risk Prevention

Although there are many differences between smart contracts and traditional contracts in terms of format, confirmation and consent, execution efficiency, payment methods and fees, etc., smart contracts can be tangible expressions of the content contained in them and can agree on the rights and obligations of the parties in the form of digital code, which is still essentially a contract. In today's traditional contract regulation has been so perfect, how to deal with the relationship between smart contracts and traditional contracts will be a matter of concern for all parties to the contract, in terms of legal, technical and management mechanisms, the use of smart contracts in advance of the applicable regulations, technical loopholes and management methods embedded in them to prevent and control risks.

4.1 Improvement of Smart Contract Provisions

First, we should clarify the extension of the contract. The Chinese civil law does not exclude smart contracts from the provisions of the contract, and it is recommended that

the conditions for smart contracts to fall within the scope of the contract should be stipulated in the law.

Second, the programming language and logic of the smart contract standardization work. Third, to clarify the rules of electronic agents of smart contracts. The agent qualification will be extended to the electronic agent, with the agency mechanism, the agent subject and agent responsibility rules, applicable to the smart contract, if the provider of the smart contract itself no problem, the electronic system defects loopholes, the third party shall be held responsible. Fourth, the relief of the smart contract is clear. If there is a problem in the process of performance, the relief can be as soon as possible. Although the contract can not be suspended, but can be improved after the completion of performance, the return to the original mechanism.

4.2 Special Rules for Smart Contracts are Standardize

First, the full use of the meaning of the independent interpretation rules. For the smart contract should make clear rules of interpretation. The nature and purpose of the behaviour of smart contracts can also become the content of the contract interpretation, can be based on the results of the implementation of smart contracts to explore the purpose of the parties to conclude a smart contract to interpret the contract.

Second, to make up for the withdrawal of smart contract offer and commitment and revocation of the application [8]. Smart contract offer and commitment although difficult to withdraw and revoke, but not beyond the scope of the contract, did not damage the autonomy of meaning. The technical characteristics of smart contracts are also their advantages, smart contracts are established under the premise of full respect for party autonomy. In general, it is necessary to standardize the management of the whole process of smart contracts from formation to performance.

4.3 Technical Restrictions on Self-performance Clause

Smart contracts need to distinguish between automatic and non-automatic performance clauses. Automatic performance creates an obstacle to contract changes and has the problems of increasing transaction costs and reducing the ease of transactions. Therefore, the necessary scenarios should be set up in the automatic performance clause to ensure the smooth operation of smart contracts through laws and industry regulations, and to provide contract rooms with a clear obligation to inform the contracting parties. The automatic mandatory performance function of smart contracts looks perfect, but when the internal algorithm of smart contracts is completely out of control, it is difficult to make people trust. Technical restrictions on self-performance clause can fix the crisis of trust caused by the uncontrollability of smart contracts.

5 Conclusions

Based on the characteristics of smart contracts, contracts rely on digital code forms, which are embedded by one party and can be quickly executed by the other party after

approval. The automatic execution mechanism of the contract brings efficiency to economic development, and it can be used to embed various conditions and assets into the blockchain through blockchain code technology to form smart terms or smart assets, and with the development of technology, smart contracts are expected to achieve significant development in various fields. However, in terms of practice, the research on smart contracts is still far from adequate. In this regard, the legal nature, risks and risk prevention and control of smart contracts have been sorted out, and it is believed that they should be regulated under the existing contract framework, and the existing terms should be broadened, and those that cannot be regulated should be explained appropriately, but only the rule of law, technical prevention and control and management mechanism have been discussed from a macro perspective corresponding discussion has not been carried out in detail. With the development of technology and the further application of smart contracts in various fields, it is conceivable that they will no longer be an occasional form of application in addition to traditional contracts, but will become a normal mode of contract formation, which requires further detailed study of the related risks.

Acknowledgements. This study is funded by the Science and technology program of China Jiliang University (2021YW98). This study is one of the phased achievements of the fund.

References

1. Bhargavan K, Delignat-Lavaud A, Fournet C, et al. (2016) Formal verification of smart contracts: Short paper[C]// Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security. ACM, 2016: 91–96.
2. Chen J D. (2019) The legal structure of smart contract. Orient Law, 2019(3): 18
3. Coblenz M. (2017) Obsidian: A Safer Blockchain Programming Language[C] In proceedings of 2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C). ACM.
4. He X, Qin B, Zhu Y, et al. (2018) Spesc: A specification language for smart contracts[C]//2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC). IEEE, 2018, 1: 132–137.
5. Hirai Y. (2017) Defining the ethereum virtual machine for interactive theorem provers[C]//International Conference on Financial Cryptography and Data Security. Springer, Cham, 2017: 520–535.
6. Lauren Henry Scholz. (2017) Algorithmic Contracts, Stanford Technology Law Review, Vol.20, 2017, p.160.
7. Nakamoto S. (2008) A peer-to-peer electronic cash system [J]. Bitcoin. https://bitcoin.org/bitcoin.pdf, 2008.
8. Regnath E, Steinhorst S. (2018) SmaCoNat: smart contracts in natural language // 2018 Forum on Specification & Design Languages (FDL). Garching, 2018: 5
9. Szabo N. (2002) Smart contracts: building blocks for digita l markets [J/OL]. Public Networks.
10. Szabo N. The Idea of Smart Contracts (1994) [J/OL]. Public Networks. http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html