ISSN: 2688-9323

Analysis on the Path of Avoiding Transaction Default Behavior by Smart Contract Technology

Xirong Gao, Ping Wen

School of Economics and Management, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

Abstract

In view of the frequent occurrence of traditional transaction default behavior, this paper explores the mechanism path of introducing intelligent contract technology to avoid default behavior. Blockchain-based smart contracts are characterized by automatic execution and non-tamperability. Buyers and sellers can write transaction guarantee assets into contracts, and one party defaults to transfer their guarantee assets directly to the other party's account. By integrating the trading process under the traditional mode, analyzing the transaction default behavior and its causes, and finally using the smart contract characteristics to design the trading process based on the intelligent contract, thereby avoiding the breach of contract, reducing the occurrence of default in the transaction and creating a good market trading atmosphere.

Keywords

smart contract; default avoidance; blockchain.

1. Preface

Although China is currently taking a series of measures to solve the problem of difficult judicial enforcement and has achieved certain results, there are still a large number of enterprises that have not fulfilled their corresponding obligations in accordance with court decisions. Under the traditional transaction method, if one party breaches the contract, the judicial approach cannot protect the rights and interests of the breached party. Early smart contracts usually couldn't have complex logic. Ethereum, as the world's first public blockchain with a built-in Turing complete programming language and the formal introduction of smart contract concepts, is currently the most popular smart contract development platform. Blockchain-based smart contracts have characteristics such as immutability and automatic execution. Smart contracts can be flexibly embedded with various data and assets, helping to achieve secure and efficient information exchange, value transfer and asset management. Blockchain smart contracts are digitally controlling valuable properties in the real world . If it is applied to credit transaction behavior, it can effectively avoid default behavior and protect the interests of both parties in the transaction. Blockchain smart contracts contain the parties' unanimous meaning or offer promises, which can be based on the contract structure or traditional contracts that are integrated and juxtaposed. Most blockchain smart contract application practices use smart contract platforms or DAPPs. They often use unified and integrated smart contracts. The template is for users to use . Smart contract templates are designed to support the management of the entire life cycle of smart legal contracts. Even if there is a dispute, they are also conducive to the automatic execution of the contract and provide a direct link with relevant legal record documents . The text of the smart contract also includes the password hash string of the legal contract. If there is a problem with the smart contract, the problem can be solved through the legal contract .

ISSN: 2688-9323

The main research contents of this article are as follows: Section 1 summarizes and reviews the current status of China ’s judicial system construction and implementation, research on smart contracts and its application status; Section 2 analyzes transaction default behaviors and causes under traditional models; Features establish a smart contract breach avoidance mechanism; Part 4 sets up the entire transaction process from signing to execution based on smart contracts; Part 5 summarizes the research.

2. Literature Review

2.1. Current Situation of China's Judicial System Construction and Implementation

In order to solve the problem of difficult implementation, China has roughly gone through three stages, and the main task at this stage is to basically solve the difficult implementation. The Supreme People's Court, the United Nations National Development and Reform Commission, and more than 60 units have established a credit disciplinary network to form a credit disciplinary system that is jointly developed by multiple departments, industries, and methods. Promote the construction of social integrity system . The amendments to the Civil Procedure Law of the People's Republic of China in 2007 established the system of the list of people who have breached trust, and provided a legal basis for the implementation of the method of disclosing information about the trustees of the trustee in judicial practice . However, there are still some problems with the current system of list of dishonest persons to be enforced, such as the lack of a complete dishonesty rating system, the lack of clear accountability for the wrongly included list, and the lack of stipulated compensation procedures and supervision procedures for those who are wrongly included in the list. Absence, the list deletion procedure is too brief, etc. . After the publication of the list of dishonest persons who made the breach, the cases that can be closed accounted for only 10% of the published dishonesty list, and a large number of cases have not been implemented .

2.2. Smart Contract and its Application

Smart contracts were first proposed by Nick Szabo, defining them as "a smart contract is a set of commitments defined in digital form, including an agreement on which contract participants can execute these commitments”. In 2008, Satoshi Nakamoto proposed the blockchain, which is a decentralized shared ledger that combines data blocks in a chain in a chronological order into a specific data structure, and ensures that it cannot be tampered with and forged.. In January 2016, the British government released a special research report on blockchain ; in December of the same year, the Chinese government included blockchain technology in the "Thirteenth Five-Year Plan" National Informationization Plan , aiming to strengthen the new The basic research and development and cutting-edge layout of the technology; in February 2017, the European Parliament pointed out in the report "How Blockchains Change Our Lives" that smart contract technology is the most potential blockchain application.

3. Analysis of Transaction Defaults and Causes

3.1. Trading Process in Traditional Mode

The existence of each subject is not independent, and it is necessary to conduct material exchanges with other subjects in order to survive and develop. At present, when conducting transactions between entities, it can be roughly divided into two phases, signing and performing.

In order to ensure the smooth progress of the transaction as much as possible, and to protect the interests of the buyers and sellers, there are about three steps in the signing phase. The first

ISSN: 2688-9323

step is to conduct market surveys to understand the market according to their own development needs, to prepare a preliminary list of cooperation objects, and to review the cooperation objects and samples in the list to further determine the cooperation objects. In the second step, the buyers and sellers conduct negotiations to Negotiate and determine the content, such as the price of the transaction, payment period, location and method, etc., and improve the details of the contract. If the company has a legal department, its legal department will review the overall content of the contract. If there is no legal department, it will seek Outside parties help to review the terms of the contract; finally, after the contract has been approved by both parties, the buyer and the seller formally sign the contract, and the contract is made in two copies, one for each buyer and seller, for subsequent certification.

After the buyer and the seller have successfully signed the contract, they need to perform according to the content of the contract, that is, they enter the performance phase, which has about four steps. In the first step, if the contract stipulates that the buyer must pay a deposit in advance, after the contract is signed, the buyer should pay the seller at the prescribed time, method and amount. If the contract does not have this clause, skip this step. In the second step, during the performance period stipulated in the contract, the seller shall deliver the contract transaction goods to the buyer in a fixed manner in accordance with the terms of the contract and in a fixed manner. In the third step, after receiving the goods from the seller within the contract period, the buyer should carefully check the quantity and quality, and give an acceptance certificate after confirmation. And jointly negotiate a solution. Finally, if both the buyer and seller are very satisfied with the transaction, the transaction ends after the buyer has successfully paid the remaining balance; if a dispute arises during the transaction, the buyer and the seller should first negotiate to resolve it. , Litigation and other methods to resolve the transaction after the dispute is resolved.

Before or after the establishment or signing of a contract, the information held by both market participants is asymmetric, and this relationship is a principal-agent relationship. According to the principal-agent theory, when buyers and sellers communicate, one party cannot grasp all the information of the other party, including their needs, purposes, and current financial status. Reaching an agreement without fully understanding the other party will lead to an increase in the default rate and affect normal operation.

When a buyer and a seller sign a contract in a transaction, it is impossible to fully grasp all the information of the other party, so there is a principal-agent theory. After the seller and the buyer have successfully signed the contract and entered the implementation phase, they are affected by various subsequent factors, and they want to maximize their own interests and ignore the other party ’s interests. Therefore, the contract signed will inevitably lead to disputes or breaches of contract. By analyzing the transaction process under the traditional model, transaction defaults can be divided into three categories: complete non-performance, incomplete performance, and delayed performance, as shown in Table 1.

ISSN: 2688-9323

Table 1. Trading defaults

Default Type / Breaching party	No compliance at all	Incomplete performance	Delayed performance
Seller	Failure to send the goods to the buyer	1. The quality of the goods does not agree with the contract; 2. The delivery form does not agree with the contract	Shipment of goods after the agreed performance period
buyer	1. Refuse to sign after receiving the seller's goods according to the contract; 2. No payment is made after signing the seller's goods	1. Pay part of the payment after receiving the seller's goods; 2. The payment method does not match the agreement	1. After receiving the seller's goods as stipulated in the contract, they did not sign for the contract during the performance period; 2. Failure to pay the payment within the prescribed period after receiving the goods

Complete non-performance refers to the behavior of the buyer and seller or one party who have failed to perform any of the terms of the contract and refused to perform it after the contract was signed. Including the seller's refusal to send the goods to the buyer, or the buyer's refusal to sign for receipt of the contracted quantity and quality of the goods, or refusal to pay for the goods after receipt. This kind of breach of contract has a greater impact on the breached party because the breaching party does not perform its obligations in the contract.

Incomplete performance means that after the contract is signed, both the buyer and the seller or one party fail to perform in accordance with the content of the contract when performing the contractual obligations. The seller's incomplete performance is manifested in the issue of only a part of the goods, the quality and quantity of the goods or the form of delivery are inconsistent with the agreement, and the buyer's incomplete performance is manifested in the payment of only a part of the payment or the payment method is inconsistent with the agreement. Incomplete performance due to issues such as the number of shipments, defective quality or insufficient payment, inconsistent payment methods, etc., the losses caused to the breached party cannot be underestimated, and in some cases, losses caused by total non-performance similar.

Delayed performance refers to the behavior in which the debtor fails to perform the contractual obligations within the performance period agreed upon in the contract after the contract is signed. The delayed performance of the seller is manifested in failure to deliver the goods within the contract period, and the delayed performance of the buyer is manifested in two aspects: delayed receipt and delayed payment. The delayed performance of one of the buyer and the seller leads to the failure of the other party's contract purpose, which is a serious breach of contract and the loss to the breached party is relatively large.

Even if the dispute is finally resolved with the assistance of law, such as the seller delaying delivery or the buyer refusing to pay, the efficiency of the transaction will be greatly reduced.

ISSN: 2688-9323

3.2. Analysis of Causes of Trading Default

The incomplete contract theory believes that due to the limited rationality of people, the incompleteness of information, and the uncertainty of transactions, the cost of clarifying all special powers is too high, and it is impossible to draw up a complete contract. Often exists. Its incompleteness manifests itself in a complex and very unpredictable world where it is difficult for people to think too far and make plans for various situations that may occur; even if a single plan can be made, the parties are very It is difficult to reach agreement on these plans, because it is difficult for them to find a common language to describe various situations and behaviors; even if the parties can plan and negotiate for the future, it is difficult for them to write down the plan in the following way: In the event of a dispute, external authorities, such as the courts, can clarify what these plans mean and enforce them.

Through the analysis of the three types of default behaviors, find out the cause of these default behaviors. According to the default motivation of the transaction subject, the causes of the breach can be divided into two categories: intentional non-performance and unintentional non-performance, as shown in Table 2.

Table 2. Causes of transaction defaults

Intentional non-performance	Capable	Some transaction entities want to invest funds such as deposits and payments through non-performance of contracts, or expect to obtain debt discounts by delaying performance, thereby occupying the interests of other parties to the transaction.
		Due to changes in market conditions, the prices of factors of production or products have risen sharply, and the parties are unwilling to continue to perform the contract, resulting in non-performance of the contract.
		Because the content or form of the contract was not clear and specific, the parties in the transaction wanted to use this as an excuse to fail to perform the contract.
	Insolvency	Some transaction entities do not have the ability to perform the contract when they sign the contract, and they want to achieve their own purpose by signing the contract, resulting in the contract being unable to perform.
Unintentional non-performance	Capable	Due to related personnel management issues, the parties to the contract forgot the contract, which resulted in the contract not being performed.
	Insolvency	The transaction subject went bankrupt due to mismanagement, etc., and the assets were insufficient to pay off the debts when the debts were settled, resulting in the contract being unable to be performed.
		The product was suspended due to problems with production factors such as technology, raw materials or equipment, and the seller could not deliver the contract product, resulting in the contract being unable to perform.
		Due to changes in market conditions, the prices of factors of production or products have risen sharply, and the parties have no ability to continue to perform the contract, resulting in the contract being unable to perform.
		In the event of a force majeure such as a natural disaster, the transaction entity is unable to deliver the product or pay the payment, resulting in the contract being unable to perform.

ISSN: 2688-9323

3.2.1. Intentional Non-performance

Intentional non-performance refers to the behavior of one party to a contract that is unwilling to continue performing the contract for various reasons after the signing of the transaction contract, causing losses to the other party. It can also be divided into two cases: performance and non-performance based on the performance of the defaulting party.

The ability to perform the contract but intentionally not performing it is the most common problem in the current traditional mode of trading, and it has the largest and worst impact on the trading market. After signing a contract, many transaction entities want to take the interests of others and make a decision to breach the contract due to various subsequent factors. The causes of performance but intentional non-performance can be divided into three types, namely, the desire to illegally occupy the interests of others, market environment factors, and the content or form of the contract are ambiguous and unspecific.

Intentional non-performance of the contract and it does not have the ability to perform. This situation mainly refers to the situation in the early signing stage, where some transaction entities do not have the ability to perform, but they want to achieve a certain purpose by signing the contract. . According to the principal-agent theory, the information content of buyers and sellers at the time of signing a contract is not completely symmetrical, and one party cannot fully grasp the other's motivations and operating conditions, so a transaction subject that does not have the ability to perform the contract will sign a contract. Some transaction entities may sign the contract in order to ease their current situation through this cooperation and achieve their ability to perform through subsequent operations. Some transaction entities will also be prepared for breach of contract when they sign the contract, but just want to pass this agreement. The second cooperation eased the current pressure and expanded other aspects of the business, which ultimately caused the contract to fail to perform.

3.2.2. Unintentional Non-performance

Unintentional non-performance refers to a situation in which one party to a contract has no intention after the transaction contract is signed, but the contract cannot be performed due to various reasons, resulting in losses to the other party to the contract. Among them, performance capability means that the non-performing party has the ability to perform, but has no intention of not performing the contract; non-performance capability refers to the non-performing party's inability to perform the contract.

An act that has the ability to perform but has no intention of non-performance is only the case where the non-performing party forgets the contract. Due to the management of related personnel, the parties to the contract forget the contract and the transaction subject fails to perform the corresponding obligations.

There are four main causes of unintentional non-performance due to inability to perform, namely bankruptcy of the transaction subject, product shutdown, changes in market conditions and force majeure factors. This kind of situation is mainly caused by poor management and management or external influence after the contract is signed.

At present, buyers and sellers conduct transactions. In order to ensure the smooth progress of the transaction, the two parties have signed a contract, which states the two parties' respective identities, rights and obligations, in duplicate and kept separately. Although the contract provides some guarantees for the smooth progress of the transaction, there are also some shortcomings. Even in some cases, the contract will lose its binding effect, such as ambiguity in the contract or contract loss.

ISSN: 2688-9323

4. Smart Contract Breach Avoidance Mechanism

A smart contract is a set of promises defined in digital form, including an agreement on which contract participants can execute these promises. The digital form means that the contract has to be written in computer-readable code. As long as the parties reach an agreement, the rights and obligations for the establishment of a smart contract are automatically performed by a computer or computer network. Through the smart contract method, the asset or currency is transferred to the program. The program runs this code and automatically verifies a condition at a certain point in time. It will automatically determine whether the asset should go to one account or return to another account. Smart contracts have the characteristics of mortgage asset guarantee, blockchain tamper resistance, automatic contract execution, and contract replenishment, which can guarantee the smooth execution of contracts, as shown in Figure 1.

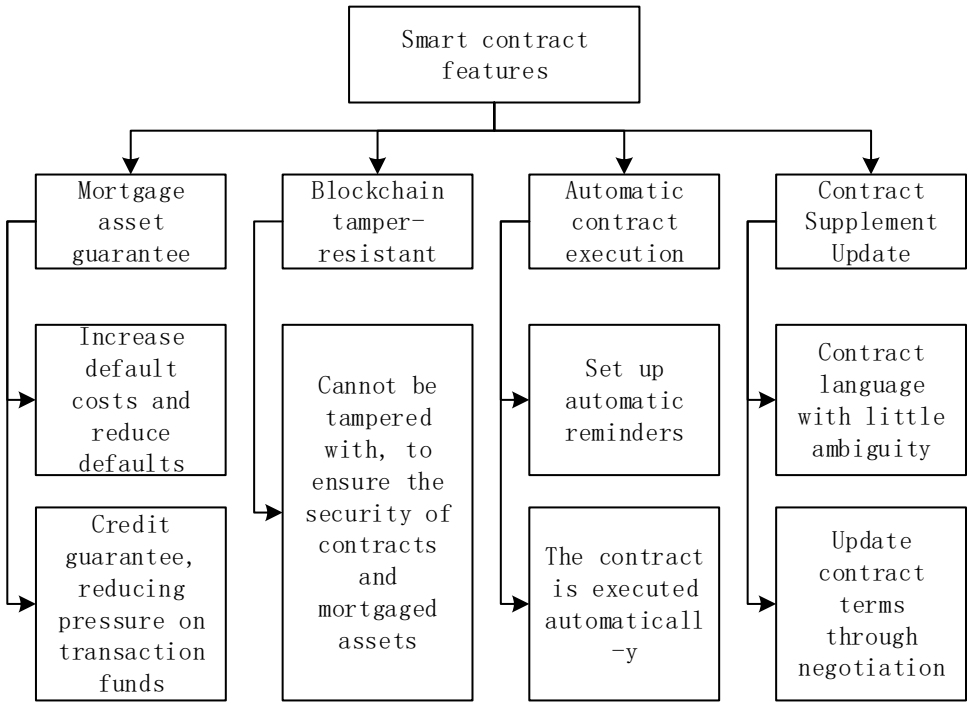

Figure 1. Smart contract features

4.1. Mortgage Asset Guarantee

Because the smart contract can automatically go to an account according to the contract content when the contract is executed, in order to ensure the smooth execution of the contract and prevent any party from defaulting, when the transaction is written into the smart contract, both the buyer and the seller must deposit A certain amount of traders mortgage assets to ensure that they can issue goods or pay for goods according to the contract. However, for the transaction subject, the mortgage asset is not only the protection of the transaction, but also a heavy financial burden. In order to reduce or avoid the financial pressure on the trader to mortgage the asset, a credit scoring mechanism is introduced in the smart contract system. Assets will be subject to a certain discount treatment based on credit scores. The higher the credit score, the greater the discount on mortgage assets, and the less mortgage assets need to be deposited during the transaction. If one party defaults, the previously written mortgage assets of the trader will be auctioned through the court, and the auction money will be used to directly compensate the defaulted party, reducing the losses brought to the defaulted party due to one party's default.

ISSN: 2688-9323

4.2. Blockchain Anti-tampering

The blockchain uses encryption algorithms such as Hash encryption and Markle tree to prevent the content in the block from being changed, ensuring the authenticity of the content and the security of the mortgaged assets of the trader. Relevant information such as the basic situation, transaction status and financial information of each merchant is included in the credit information system. The relevant information uses the blockchain time stamp and password technology to ensure that it can be updated but cannot be tampered with.

The transaction subject uses a smart contract to sign a contract. After the contract is completed, the entire transaction record will still be recorded on the blockchain. By querying and collecting the corresponding transaction record, it can grasp its basic business scope, financial status and other basic information. As a basis for transaction credit scores. Before signing a contract, the transaction subject can inquire about the other party's relevant information through the credit information system, and understand the other party's transaction credibility, the purpose of the contract, and the possibility of timely performance of the contract through information analysis to provide guarantee for the successful implementation of the contract. Smart contracts are stored and deployed in the blockchain network, and the nodes in the network are independent of each other and all have the same copy, so the content of the contract is almost impossible to be tampered with. At the same time, the contract execution records are also kept in the blockchain, which can be used as Permanent transaction proof. Blockchain anti-tampering can avoid defaults caused by intentional non-performance and ability to perform.

4.3. Automatic Contract Execution

When the smart contract is written, an automatic reminder function is added. The transaction subject can set the reminder time and frequency. The system will send a reminder to perform the contract in a timely manner according to the set time and frequency to avoid the causes of breach of contract that has the capability to perform but has no intention of not performing.

Because of the automatic execution of smart contracts, when the contract is signed, both the buyer and the seller write into the trader's mortgage assets at the same time. After one party defaults, their mortgage assets are automatically transferred to the other's account to protect the interests of the other party and reduce economic losses caused by one party's default . The creation and execution of smart contracts depend on the blockchain protocol, so the coercive force of the contract can be guaranteed. In order to prevent a party from defaulting after the contract is signed, the transaction subject is required to deposit a certain amount of liquidated damages in the system in addition to the transaction amount when signing the smart contract to ensure the successful performance of the contract. Regardless of whether the transaction subject has defaulted, the smart contract will pay the corresponding transaction amount or liquidated damages in accordance with the contract terms to ensure the interests of all parties. When there is a dispute in the transaction, no external intervention is required, and the smart contract can complete the entire transaction according to the term code written in the implementation, effectively ensuring the transaction efficiency. In order to avoid defaults caused by intentional non-performance and ability to perform.

4.4. Contract Supplement Update

The terms of the smart contract are determined by the code. Because of the clarity of the logic of the code, it is less prone to ambiguity than natural language. After the smart contract is signed, both parties to the transaction can update the agreement in real time after negotiation or in accordance with the law to redistribute the mortgaged assets, payment, and goods of the trader.

Willing to perform but default due to inability to perform. As the contract was written into the mortgage assets of the trader at the time of signing the contract, if the contract cannot be performed, the mortgage assets will be directly transferred to the court's auction process.

ISSN: 2688-9323

Compensate the defaulted party. If the auction proceeds exceed the purchase price of the transaction, the excess amount will be returned to the defaulting party's account. In the event of a breach of contract due to force majeure factors such as natural disasters, a supplementary contract can be signed after the two parties have negotiated or according to legal provisions to return all or part of the mortgaged assets. Therefore, this feature can avoid breach of contract caused by unintentional non-performance and inability to perform, and can protect the interests of the loser when force majeure occurs.

5. Smart Contract Transaction Process

5.1. Smart Contract Transaction Initiation and Signing

The initiation and signing of a smart contract require three main bodies: a smart system, a contract initiator, and a contract responder.

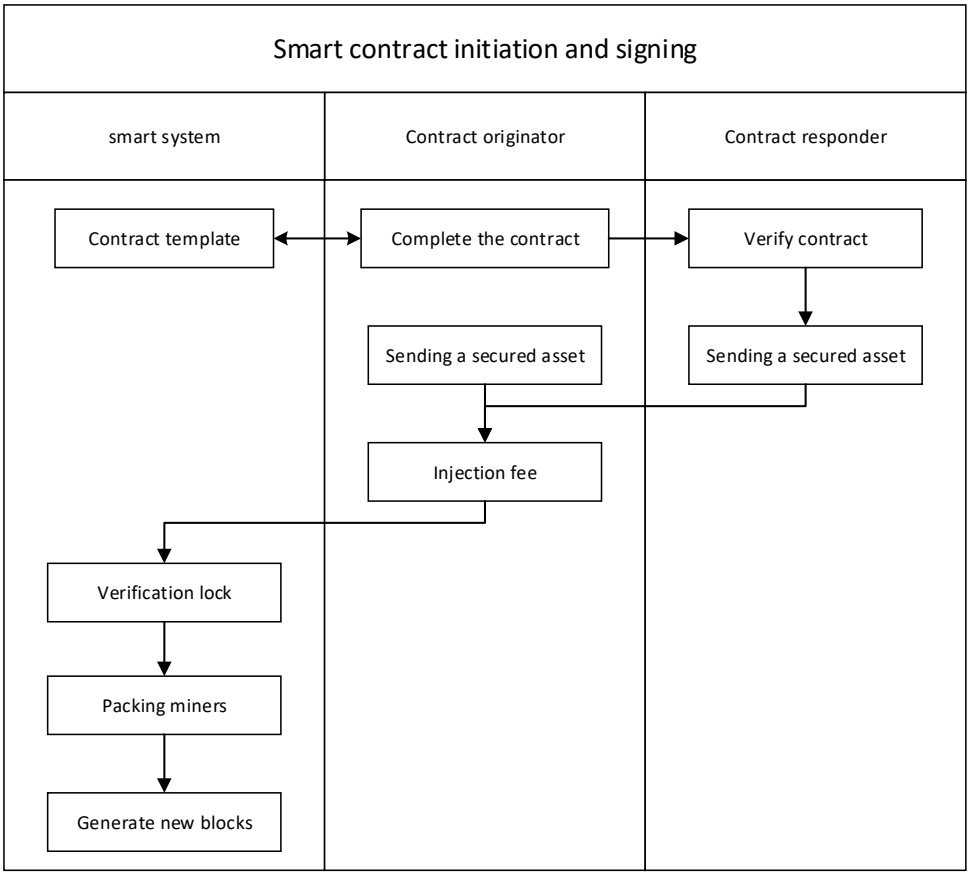

Figure 2. Flow chart of smart contract transaction initiation and signing

First, the contract initiator completes the content of the contract through the contract template and open API provided by the intelligent system. At the same time, the contract initiator can also set up a new contract template based on the contract content, and the contract responder verifies the contract content terms. After the terms and conditions of the contract are verified, the contract responder and the initiator send the mortgaged assets of the trader to the intelligent system, and the contract initiator needs to write the contract fee. After the transaction fee is written, the verification node in the smart system verifies and locks the smart contract and the mortgage asset sent by the trader. Finally, the accounting miner in the intelligent system packages the verified contract, and subsequently generates new blocks, and the consensus is solidified. The smart contract is successfully recorded in the intelligent system and waits for execution. The entire network can see the contract.

ISSN: 2688-9323

5.2. Smart Contract Transaction Execution Process

The execution phase of the smart contract is mainly that the verification node in the smart system judges whether the contract should be executed according to the externally input conditions to be verified, and the execution content is executed according to the provisions.

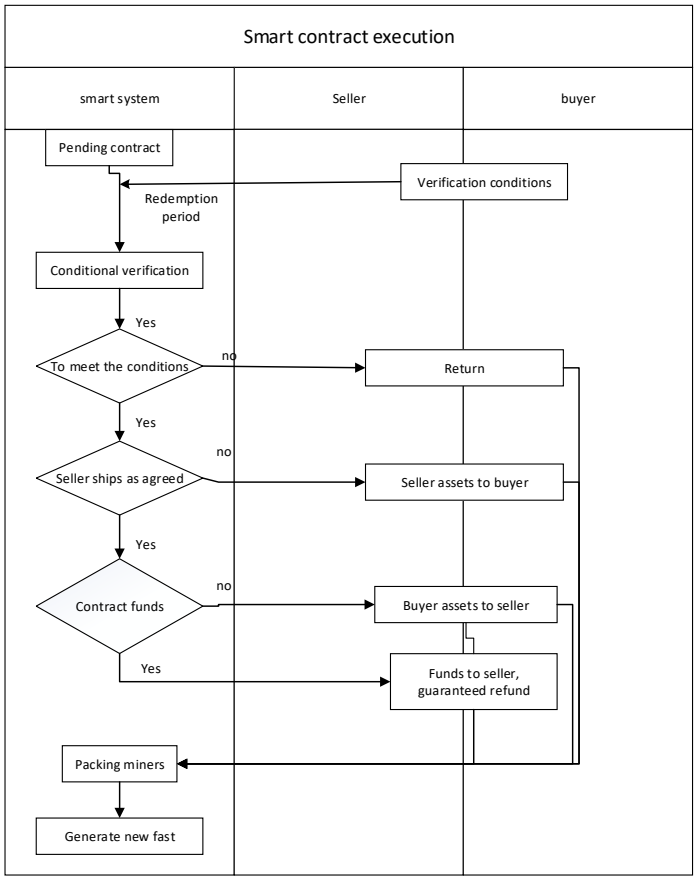

Figure 3. Flow chart of smart contract transaction execution

After the smart contract is successfully solidified by the consensus, before the redemption period is reached, buyers and sellers can enter the conditions to be verified, which is convenient for the verification node to verify whether the conditions for contract execution have been reached. After the redemption period is reached, the verification node verifies the entered verification conditions and executes the contract according to the terms of the contract. If the contract does not meet the conditions for execution, the contract funds and the encumbered assets are automatically returned to their original owners; if the seller fails to send the goods to the buyer in accordance with the contract, the seller's mortgaged asset is automatically transferred to the buyer's account; if the seller sends the goods in accordance with the contract terms , But the buyer did not pay the purchase price in accordance with the contract, and the buyer's mortgaged secured assets were automatically transferred to the seller's account; if the buyer and the seller successfully transacted, the seller sent the goods in accordance with the contract, and the buyer paid the payment in accordance with the contract. Accounts; finally, the bookkeeping miners package the contract execution status, and subsequently generate new blocks. Regardless of whether the contract is successfully executed, the fees generated during the period will be automatically deducted to the consensus node or the bookkeeping miner and will not be refunded.

ISSN: 2688-9323

6. Conclusion

Due to the low default cost of traditional transactions, in order to maximize their own interests, the transaction subject always has a motivation for default. The more unstable the market economic conditions, the larger the transaction amount, and the greater the default probability of the transaction subject, which will have a greater adverse impact on the entire industry and the entire market. This article integrates the transaction process under the traditional model and analyzes two types of six types of transaction defaults. It is found that buyer defaults are concentrated in the two stages of confirming receipt and payment, and seller defaults occur in the delivery stage; the reasons for the default behavior of the transaction subject Can be divided into two categories of intentional non-performance and unintentional non-performance, each of which can be divided into two cases with or without the ability to perform the contract. Aiming at the causes of the four types of default behaviors, a smart contract evasion mechanism is proposed, which uses the four characteristics of smart contract mortgage asset guarantee, blockchain tamper resistance, automatic contract execution, and contract replenishment to evade the causes of default. Finally, according to the technical characteristics of smart contracts, a process for initiating, signing and executing smart contract transactions is formulated. This will increase the probability of contract performance and reduce the occurrence of defaults.

References

[1] Bartoletti M, Pompianu L. An empirical analysis of smart contracts: platforms, applications, and design patterns[J]. Proceedings of the International Conference on Financial Cryptography and Data Security. Springer, Cham,2017:494-509.

[2] Wood G. Ethereum: A secure decentralized generalized transaction ledger (EIP- 150 revision) [EB/OL] . 2013 [2018-11-2]. http:/ /gavwood.com/ paper. Pdf.

[3] William Mougayar, The Business Blockchain: Promise, Practice and Applications of The Next Intermet Technology.[M]. Wiley, 2016:42.

[4] See Christopher D.Clack,Vikram A. Bakshi & Lee Braine, Smart Contract Templates: Foundations, Design Landscape and Research Direction [EB/OL].(2016-08-04) [2018-11-12]. https:// arxiv. Org /pdf/1608.00771v2.pdf.

[5] Szabo N. Formalizing and securing relationships on public networks [EB/OL].1997[2018-6-04]https://firstmonday.org/ojs/index.php/fm/article/view/548/469.DOI:http:/dx.doi.org/10.5210/fm.v2i9.548.

[6] Nakamoto S. Bitcoin: a peer-to-peer electronic cash system[EB/OL].(2016-8-04)[2018-6-04] https:/ /bitcoin.org/bitcoin.pdf .

[7] JanuaryHancock M,Vaizey E. Distributed Ledger Technology: beyond block chain [EB/OL]. 2015 [2018-07-19].

[8] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf.