

Investigating the mechanism of concluding smart contracts and the operation of smart contracts in financial markets in the context of blockchain

Reza Mashhadizadeh
PhD student in Financial Engineering

Submit: 16/02/2021 Accept: 05/04/2021

Abstract

The growth of technology with the creation of new tools for exchanges in financial markets has led to the development of e-commerce. The tools used in financial markets are blockchain and smart contracts. This study seeks to answer the question of whether smart contracts are legally valid contracts and if they are considered valid, what is their function in the financial markets? Smart contracts are contracts that are concluded on a blockchain platform under the supervision of artificial intelligence and are based on digitally encrypted currencies. Contracts are considered subject to the general rules of contracts due to the non-approval of special laws in different legal systems, and according to the principle of contractual freedom, they are considered valid contracts. Through studying the legal system of the United States of America, seeks to state that the main applications of smart contracts and blockchain header in financial markets are the transfer of different types of tokens, creating transparency and security in transactions in financial markets, and the sale of securities. Digital, syndicated loans, cash stocks and Commercial is a protection loan.

Having these blockchain platforms has created transparency in supply chain-based exchanges and prevented financial abuses. This article in two sections generally first examines the mechanism of concluding smart contracts and then examines the function of smart contracts in financial markets.

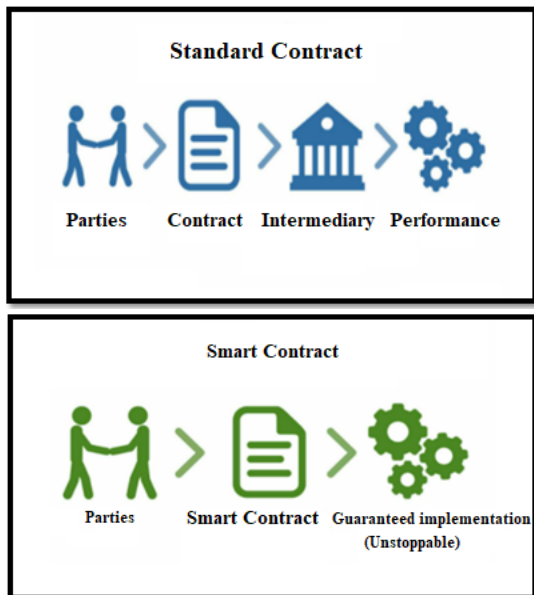
Also, the relationships between effective blockchain indicators to improve the competitiveness of the food industry and the effect of smart contracts on this industry have been studied.

Keywords

Smart Contract, Blockchain, Food Supply Chain, Exclusive platform, Oracle, Contract protocols.

1. Introduction

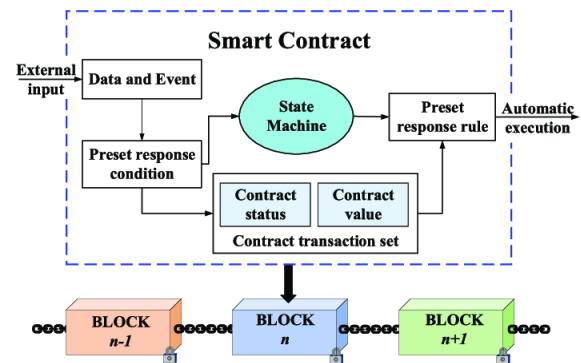
Smart contracts are a programming code that are implemented on the blockchain. They execute specific commands given by the programmer in the event of a series of parameters. Smart contracts are a new method that eliminates the need for us to trust others. A typical contract, on the other hand, is an agreement between two or more persons that binds them to a future obligation. For example, a contract for renting a house in exchange for paying a rent. For example, when you purchase a file from the Internet, there are codes behind, that are defined for them. If the user paid and the amount was enough, show her the link to download the file, otherwise show an error message.



What sets smart contracts apart from regular ones is the use of blockchain technology, which eliminates the need for us to trust intermediaries. In other words, the smart contract is a code that is activated on the blockchain to check and execute the terms of an agreement between the two parties without the need for intermediaries. When a smart contract runs on a blockchain platform, it is unstoppable and no one can stop it. With smart contracts, you can create programs

and projects that will continue to work forever without any intermediaries and disability. These programs are also called decentralized programs. Even a smart contract developer cannot change the smart contract code registered in the blockchain. Aside from complex technical processes, when a smart contract is signed on the blockchain, it is shared among all members of the blockchain, or nodes, and everyone will have a copy of it.

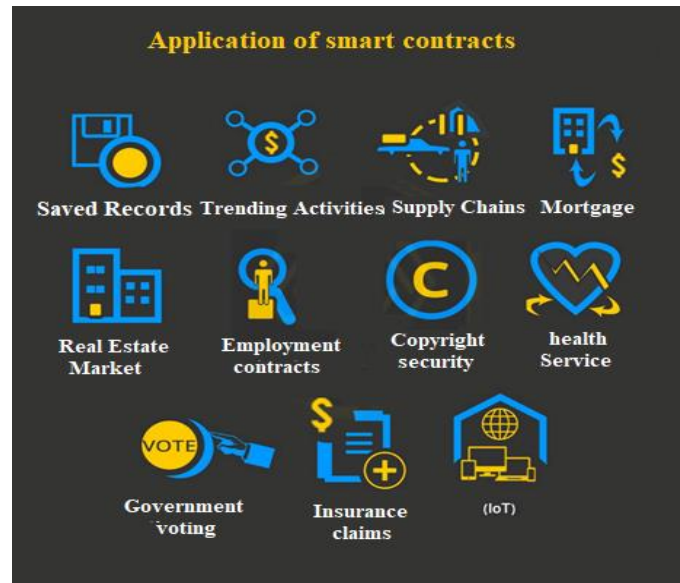
Therefore, it is almost impossible to prevent or manipulate it because all members of the blockchain are running it, not one or more specific servers and centralized entities.



Uses of smart contracts

Smart contracts are formed as a result of the evolution of blockchain, which helps you to exchange money, assets, stocks or any valuable things in a transparent manner, without the need for the assistance of intermediary service providers.

Setting up a smart contract provides a unique way to solve problems, including trust accounts, insurance, government processes, and more.



Terms of the contract

The terms of the smart contract are precisely the sequence of operations that, if the conditions occur, lead to the execution of the contract. These conditions must be specified by programming. The parties to the contract must sign these terms.

Oracle

Oracle refers to something that provides external information to a contractor to process their contract. For example, if Oracle is going to review the meteorological information contract, it could be a meteorological site.

Oracles may mislead the smart contract by hacking or modifying the reference site information.

The idea of oracles has been around for several years and there have been discussions about how to implement and trust them.

Oracle retrieves and validates external resource data through web APIs and market data segment for smart blockchains and contracts. The data that smart contracts require includes information such as prices,

weather or even creating a random number for gambling.

The oracles are located between the blockchain and the data sources and provide the information required by the blockchain by performing a query. Therefore, smart contracts can be executed based on the information provided by Oracle. Data sources in real-world markets and web APIs, such as blockchain and smart contracts, are not deterministic.

Oracles act like bridges, turning this external and uncertain information into a comprehensible and workable format for blockchain.

Oracle's extraordinary ability to connect off-chain and on-chain data as an intermediary between traditional and blockchain networks has significant long-term implications. The main problem, however, is that these oracles come from centralized sources, which usually require external permissions, and this is where blockchain has a problem.

Jimmy Song provides a useful analysis of the fundamental problems of oracles and smart contracts. Oracle's challenge is more in terms of security, credibility and trust that occurs between other oracles and the unreliable execution of smart contracts. Digital

space must be aware of the physical world. Oracles play an influential role in smart contracts because the data they provide determines how smart contracts are executed.

Exclusive platform

A specific platform is issued to the smart contract in blockchain and distributed among the platform nodes. You also need an official client software that connects directly to the blockchain to sign a contract. Ethereum is currently the most popular platform for executing smart contracts.

background research

The concept of smart contracts was first introduced by Nick Szabo in the early 1990s, and her predictions about their implementation were close to reality.

Nick defined these contracts as contract protocols embedded in software and hardware that would be costly to violate. Nick Sabo unveils Vending Machine to express her design.

Initially, these devices were used to justify the efficiency of this type of contract in calculating the costs of arbitration, mediation of transactions and execution of concluded contracts. In other words, the invention of payment machines in the 90s led to the creation of a mechanism for using machines to perform mathematical calculations or conclude very simple electronic contracts. Of course, years before Nick Sabo presentation, financial institutions in the United States used computer codes in financial transactions, such as option contracts.

In 2009, the Bitcoin Protocol first used Blockchain technology, and then in 2015, the Ethereum Network was founded by a specialist named Vitalik Buterin, who implemented the first examples of smart contracts.

Earlier, the success of Bitcoin led many to equate the block with a platform for the transfer of digital currencies. But in fact, the blockchain has a wide range of applications, including the implementation of smart contracts.

Nowadays, smart contracts are mainly used in the field of currency cryptography. Decentralized virtual

currency protocols are essentially intelligent contracts that have decentralized cryptography and security.

These contracts are widely used in existing cryptocurrency networks and are one of Ethereum's most prominent features. Ethereum is currently the most popular smart contract platform, but many other digital currency blockchains (including EOS, Neo, Tezos, Tron, Polkadot) can execute them.

Mechanism of concluding smart contracts

• The concept of smart contracts

Smart contracts are decentralized agreements created in computer code and stored on a blockchain platform. These contracts are the result of long-term efforts to eliminate possible inefficiencies of traditional contracts. The technology used in smart contracts is a more advanced sequence and type than electronic data transmission technology. In addition to the ability to record information and even cryptocurrencies, blockchain also has the capacity to enter into macro financial contracts in the form of smart contracts.

Smart contracts are contracts that are overseen by artificial intelligence.

• Intelligent contract algorithms

Blockchain contracts with programming algorithms are free from ambiguity in the contract. In order to facilitate the conclusion of electronic contracts in this context, in the United States, contract models have been designed to prevent the problem of ignorance of some people in how to use programming algorithms.

These draft patterns can include different types of smart contracts. If the parties to the contract use them, they can enter into smart contracts with full knowledge of the terms of the contract and its provisions. One of the conditions for concluding smart contracts is obtaining a license to use digital signatures. Government agencies ensure the authenticity of electronic contracts resulting from digital signatures. If the signatory does not pay the damages, the government will pay the damages and until the settlement with the government, the contracting party will not be able to conclude electronic contracts. This

is one of the ways to ensure the implementation of the contract and increase its security.

- **Conditions for the accuracy of transactions in smart contracts**

A contract is a legal agreement between the parties that binds them to perform the contract. Smart contracts, like traditional contracts, have legal aspects and their validity follows the general rules of contracts due to the non-approval of special laws for the recognition of such contracts. In contract law, a valid contract must have the basic terms of the transaction.

The basic conditions of the transaction are: acceptance, transfer of contractual ownership, eligibility and legality of the transaction.

- **Problems facing smart contracts in financial markets**

Smart contracts, due to their infancy, are associated with problems in their application in any legal system. The most important challenge that a country's legal system faces in accepting such contracts, especially in the field of money and capital markets, is the issue of the validation of cryptocurrencies.

Smart contracts written on a blockchain platform are written by humans. This means that human error is always present and its existence will lead to hacking and abuse.

Similar to what happened in the 2016 attack on the Decentralized Authority (DAO). Hackers exploited a vulnerability in the organization's smart financing contract to steal funds.

The process of performing smart contracts

The process of operating smart contracts on a blockchain platform can be summarized in two processes:

- **Escrow process**

This process focuses on the mechanism for enforcing the provisions of smart contracts. In this process, after concluding and finalizing the contract, the transfer of ownership of the contracting parties and the process of registering and offering the provisions of the contract

in the blockchain platform, without any action by either party, is done by artificial intelligence.

According to this process, if the parties to the contract are more than two people, any receipt and payment by any of the parties to the other must be done with the consent of the parties to the contract through its approval by their own private keys.

- **Usage of escrow accounts**

Escrow accounts were most commonly used in real estate and stock market transactions in the past; Thus, the buyer of the property, by depositing money in the Escrow account, in addition to completing the argument for its purchase and reassuring the seller, has the opportunity to carefully review and make the necessary legal inquiries, and then to complete the payment only the custodian must pay. Transfer to seller account.

In stock exchange and stock trading, the Escrow account is more efficient. In general, stocks are often offered as securities. In this case, although the investor is the real owner of the shares. But there are restrictions on access to stock.

For example, managers who receive a certain amount of stock as compensation, are not allowed to sell the stock for a certain period of time. These shares are tactical method to retain senior executives.

Escrow account is also efficient on Internet and e-commerce. An online platform that serves as an interface for selling products online can allow the buyer to transfer the required amount to an Escrow account such as escrow.com by connecting to the escrow account service, and they can keep the money until the product is delivered. Once the product has been delivered and approved by the buyer, the online escrow account completes the transaction by paying the seller. This payment method is not commonly used and is a mechanism used for special and expensive purchases such as buying jewelry or valuable works of art.

- **Usage of escrow accounts on blockchain**

Benefiting from a trust account and escrow account services is a boon in the blockchain world, despite a third party managing digital currency payments.

You must have heard the phrase "silent money" about Fiat money, and you must know that the payments made through digital currency are untraceable.

As a result, it may be possible to use the term "invisible money" for digital currencies such as bitcoin, which not only have no language but no one can even see them physically. On the other hand, due to the decentralized nature of these types of assets, their spending and transfer is more sensitive; Thus, the concept of a trust account or an escrow account was introduced into the blockchain to facilitate trust between the parties to a transaction.

➤ **Self-help process**

This process focuses on how to operate and compensate damages from one party to the contract to the other without the need for a court judgment, according to the instructions given.

In other words, in the normal case, the process of repaying a contract in case of non-implementation of the provisions of the contract or its non-implementation in accordance with Section 6 of Clause 9 of the US Trade Uniformity Law will be done by ruling in US state courts.

However, the process of repaying a contract in smart contracts in case of non-implementation of the provisions of the contract, for example in the event of sudden expropriation by the judicial authorities, after concluding the contract, by artificial intelligence in accordance with the instructions given to it .

Of course, this does not prevent the parties from filing a lawsuit in court, and in the event of damage to the party to the contract for which no obligation has been determined, receiving compensation for her after the court ruling will be normal losses.

Conclusion

Nowadays, with the advent of data encryption technology, the latest electronic tools used in the developed world are decentralized platforms and smart contracts. The pillars of the use of these contracts in the legal system of digital signatures, cryptocurrencies, Nowadays, with the advent of data encryption technology, the latest electronic tools used in the

developed countries of the world are decentralized platforms and smart contracts.

The pillars of these contracts in the legal system are digital signatures, cryptocurrencies, blockchain, artificial intelligence and oracles. In addition to passing new laws, the issue of educating the public and monitoring the proper implementation of laws is also considered a necessity. The use of smart contracts in the Iranian legal system is also subject to the provision of programs to inform the public about how to use it and the adoption of laws regarding the obligation of individuals to conduct their transactions in the form of these contracts.

Blockchain technology has recently entered the food industry. The food industry is highly sensitive due to its direct relationship with human health. Blockchain helps increase integration and productivity in the food industry by positively impacting indicators such as traceability and fraud prevention and supply chain coordination and cost reduction. Also, the supply chain gains a competitive advantage by taking advantage of blockchain features for its stakeholders.

According to experts, traceability means the entire history of the product from the farm to the people's table. The food industry needs a reliable and transparent tracking system that is made possible by blockchain.

Research shows that tracking and fraud prevention indicators, the most effective criterion, have higher effect than other indicators. The existence of a reliable tracking system in the food industry is very effective in improving the efficiency of indicators in this area. By improving the tracking index, it is possible to reconstruct the product history at any time and place. This index has the ability to improve the quality, safety of food and prevent waste.

Smart contracts are easy to complex, difficult to maintain and secure, and have many external dependencies. The only real place where smart contracts can really be trustworthy is in decentralized digital carrier tools like Bitcoin.

What differentiates a regular contract from a smart contract is that computer code solves the problem of the need for trust. The main feature of a smart contract

is to execute it without the need for trust. Third parties will not be required to perform the various terms of a contract. Instead of relying on people who can intentionally or unintentionally make mistakes, a smart contract does exactly what it's planned and does at the right time. At present, smart contracts are not recognized by governments. So, if government agencies decide to create a legal framework for smart contracts, new issues will arise.

Ownership of a home on a smart contract is not currently accepted by governments. Smart contracts are not executed without programming. You need to have one or more skilled programmers to handle smart contracts well. Of course, there are services for creating smart contracts by ordinary users, and users will be able to set up some of their smart contracts with a few clicks. However, these services can not design complex contracts.

Reference

- 1) Leila rezai, Reza Babazadeh (1398). Investigate the relationships between effective blockchain indicators to improve the competitiveness of the food industry
- 2) Mahdi Naser, Seyyed Mohammad Hassan Razavi(1399). Legal analysis of the function of smart contracts in digital transfers in financial markets.
- 3) Seyyed Hossein Safaei (1392). Introductory course in civil law, Volume II. Mizan Publications.
- 4) Mafi, Homayoun, Kaviar, Hossein (1392). Comparative study of the law governing electronic contracts concluded in the Internet environment from the perspective of legal systems of United State of America, European Union and Iran. Journal of Private Law Studies. No1.



International Journal of Financial Technology Perspective
(FinTech)

سال (۲) / شماره (۴) / بهار ۲۰۲۵

بررسی مکانیسم انعقاد قراردادهای هوشمند و عملکرد قراردادهای هوشمند در بازارهای مالی در بستر بلاک چین

رضا مشهدی زاده

دانشجوی دکتری مهندسی مالی

چکیده

رشد تکنولوژی با ایجاد ابزارهای جدید جهت مبادلات در بازارهای مالی موجب توسعه تجارت الکترونیکی شده است. جدیدترین ابزار به کار گرفته شده در بازارهای مالی زنجیره بلاکچین و قراردادهای هوشمند می‌باشند. این تحقیق به دنبال پاسخ دادن به این سوال است که آیا قراردادهای هوشمند، قراردادهایی معتبر از نظر قانونی تلقی می‌گردند و در صورت معتبر تلقی شدن چه کارکردی در بازارهای مالی دارند؟ قراردادهای هوشمند، قراردادهایی هستند که در بستر بلاکچین تحت نظارت هوش مصنوعی منعقد و مبتنی بر ارزشهای رمزنگاری شده دیجیتال می‌باشند.

این قراردادها با توجه به عدم تصویب قوانین خاص در نظامات حقوقی مختلف، تابع قواعد عمومی قراردادها تلقی گردیده و با توجه به اصل آزادی قراردادی، عقود معتبر تلقی می‌گردند. این تحقیق با مطالعه نظام حقوقی کشور ایالات متحده آمریکا به دنبال بیان این مطلب است که عمده کاربرد قراردادهای هوشمند و سربرگ بلاکچین در بازارهای مالی، نقل و انتقال انواع مختلف توکن، ایجاد شفافیت و امنیت در مبادلات انجام گرفته در بازارهای مالی، فروش اوراق بهادار دیجیتالی، وام‌های سندیکا، سهام نقدی و بازرگانی وام حمایتی می‌باشد. همچنین برخورداری این قراردادها از بستر بلاکچین موجب ایجاد شفافیت در مبادلات مبتنی بر زنجیره تأمین و جلوگیری از سوءاستفاده‌های مالی شده است.

در این مقاله در دو بخش به طور کلی ابتدا به بررسی مکانیسم انعقاد قراردادهای هوشمند و پس از آن به بررسی کارکرد قراردادهای هوشمند در بازارهای مالی پرداخته شده است.

همچنین، به بررسی روابط میان شاخص‌های مؤثر بلاکچین برای بهبود رقابت پذیری صنایع غذایی و اثر قراردادهای هوشمند بر این صنعت، پرداخته شده است.

کلمات کلیدی

قراردادهای هوشمند، بلاک چین، زنجیره تأمین مواد غذایی، پلتفرم انحصاری، اوراکل، پروتکل‌های قراردادی