Study on the Application Scenarios of Blockchain in Futures Exchange Business

Yi-duo CHEN\textsuperscript{1,a}

\textsuperscript{1}Northeast Agriculture University, Harbin, Heilongjiang Province, China
\textsuperscript{a}cyd990716@163.com

Keywords: Blockchain, Decentralization, Futures Exchange, Business Innovation.

Abstract. The blockchain technology application scenarios in futures exchange business are studied, and solutions to existing business pain points based on blockchain technology are given. In the transaction settlement business, it is proposed to build a blockchain transaction and use DCEP as the transaction fund, which solves the problems of slow settlement speed, slow information transmission with more intermediaries, and slow circulation of funds in the transaction settlement process; in the delivery business, it is proposed to use blockchain to store monitoring data and build a trading platform for warehouse receipts, which solves the problems of safe storage of monitoring data and flow of warehouse receipts; in the supervision business, it is proposed to use blockchain technology and encryption technology to solve the problems of the irregular flow of credit funds into the futures market and leakage of customer privacy.

1. Introduction

Blockchain is an innovative application of computer technologies such as distributed data storage, peer-to-peer transmission, consensus mechanism, and encryption algorithms in the Internet era. With essential features such as decentralization, de-trust, collective maintenance, reliable database, open-source, and anonymity, blockchain technology has shown great application potential in digital currency, fund clearing, financial asset trading, securities issuance, and smart contracts\textsuperscript{[1]}. In the main business of the exchange, trade settlement, delivery, supervision and etc, there are problems such as low information transparency and complex communication links between multi-department and multi-agency. In terms of research on the combination of blockchain and exchange business at home and abroad, Tsai proposed a dual-chain structure in transaction settlement\textsuperscript{[2]} to solve the problems of information dissemination delay caused by too many blockchain nodes. Mainelli explored how blockchain technology can verify the information and test consistency in settlement and its commercial value, and they argued that blockchain technology could reduce both risk and cost\textsuperscript{[3]}. In terms of delivery business, Chuanlei Wang study the coupling relationship between blockchain and supply chain logistics information resources in three aspects, such as subject, transaction mechanism, and smart contract, to build a blockchain-based supply chain logistics information ecosystem model\textsuperscript{[4]}. In terms of regulation, Li et al. argue a dual paradox between the "decentralization" of blockchain technology and the traditional regulatory model and "Re-centralization". A limited centralized blockchain network organization structure should be adopted to achieve a balance between security, scalability, and decentralization\textsuperscript{[5]}. In this paper, from a practical point of view, we analyze the blockchain technologies that are currently more mature or even commercially available, taking into account the specific business needs, to provide some reference for the future adoption of blockchain technology by exchanges.

2. Scenario Analysis of Exchange Using Blockchain

The business scenarios of exchange transaction settlement, delivery, and market supervision, there are often problems such as low transparency of slow information circulation and high hardware and
software facilities operation and maintenance costs. This paper will analyze these problems and try to solve them with the existing, more mature blockchain technology.

2.1. Transaction and Settlement Business

2.1.1. Business Pain Points

Low fairness and reliability, high operation, and maintenance costs. Due to its monopoly status, the centralized exchange has always had the risk of power rent-seeking, and the data of the centralized system can be tampered with privately. Simultaneously, centralized servers are prone to a single point of failure and vulnerable to attacks. To improve the reliability of the trading system, it is necessary to back up servers and conduct off-site disaster recovery and establish data centers in multiple locations, which greatly increases the operation and maintenance costs.

Low settlement efficiency and high settlement costs. At present, futures settlement needs to be carried out by the futures exchange with depository banks, subordinate members, and other organizations after the market closes. These organizations then settle with their respective customers, which is a complex process with many participating parties, which is inefficient and greatly increases the settlement cost.

2.1.2. Advantages of Using Blockchain Technology

Since blockchain data is stored on the chain and cannot be tampered with, there is no need for the exchange to conduct full settlement, and members at all levels can obtain settlement data from the chain by themselves. Moreover, as long as the nodes exist, the historical settlement data can be checked at any time, and there is no need for individual members to save the data by themselves, which greatly reduces the operation and maintenance costs.

2.1.3. Scenario Application

Using blockchain technology to build a decentralized exchange, contracts and customer assets can be traded as pass-throughs, and user funds and contracts can be aggregated and settled in time during the transaction.
Figure 1. Off-chain relay, on-chain settlement.

Note: The buyer and seller under the chain will conclude the transaction, and after the transaction, the transaction data will be transferred to the smart contract, which will control the transfer of funds between accounts according to the set instructions.

2.1.4. Feasibility Analysis

Now there are more mature decentralized exchange Uniswap\textsuperscript{[6]}, decentralized trading protocol 0X\textsuperscript{[7]}, and Loopring Protocol\textsuperscript{[8]}. Among them, Loopring Protocol adopts zero-knowledge roll-up to make the transaction speed up to 1400 strokes per second, and the throughput can reach 16,400 strokes per second if the on-chain data availability is turned off, which can basically meet the needs of professional traders, market makers, and automated trading robots.

2.1.5. Potential Problems

The current trading protocols all run on public chains, and the transaction processing volume per second is still low compared to the existing trading systems. If futures exchanges consider using this method to participate in the settlement, they should use a federation chain to improve the block confirmation speed or separate the aggregation and settlement aggregation can be completed off-chain and settle on-chain after the aggregation is completed.

2.2. Settlement Business

2.2.1. Business Pain Points

The delivery business involves registration, audit, cancellation, withdrawal, and financing of electronic warehouse receipts. It needs to be participated by multiple organizations such as warehouses, banks, exchanges, and regulatory agencies, and the process is more cumbersome and
the information transparency is lower. Moreover, because the goods are stored in the warehouse for a long time, they may face various risks such as theft and damage. Modern storage depots have various sensors to monitor storage conditions, and it is more difficult to fully achieve the safe storage and anti-tampering of this monitoring information under the existing storage methods.

2.2.2. Advantages of Using Blockchain Technology

The electronic warehouse receipt based on blockchain technology can connect the futures trading error, delivery warehouse, banks, customers, and regulatory agencies closely together to promote the transparency and openness of warehouse receipt information and speed up the process. Furthermore, it can ensure the safe storage of warehouse monitoring information.

2.2.3. Scenario Application

Research and design a credible information storage and electronic warehouse receipt trading platform, store the information related to various goods in the warehouse represented by warehouse receipts and the IoT information of monitoring goods as a credible information chain and provide the underlying data platform support for the establishment of trust relationship among all participants in the supply chain and credible warehouse receipt transfer.

2.2.4. Feasibility Analysis

Interstellar cloud storage IPFS\(^9\), has basically solved using blockchain technology to store a large amount of data, such as monitoring information. Wang Wenqi et al. have designed an underlying block storage system based on Bitcoin source code that can store various information as well as suitable for transaction operations, and have designed a transaction algorithm that can trade electronic warehouse receipts\(^{10}\).

2.2.5. Potential Problems

Although the blockchain technology can be used to ensure that the data on the chain is safe from tampering, the credibility of the data deposited on the chain cannot be guaranteed, and it is still necessary to strengthen the supervision to ensure that the data deposited on the chain is true and credible.

2.3. Market Supervision Business

2.3.1. Business Pain Points

In identity verification, users' information is not interoperable among different financial institutions, requiring repeated registration and submission of sensitive personal identity information, which will bring the risk of information leakage.

Certain users may also take advantage of the lack of information flow between institutions and use credit funds and other funds that are restricted from flowing into the futures market to conduct transactions, affecting the normal financial order of the market.

2.3.2. Advantages of Using Blockchain Technology

Using encryption technology to generate a public key system that is more in line with the application of smart terminals, there is no media requirement for file storage, no privacy leakage after loss, and no risk of identity theft and impersonation as it cannot be used alone for identity authentication.

Loans issued by blockchain technology can be "dyed"\(^{11}\) to prevent them from flowing into securities and futures, real estate, and other industries that restrict access to bank credit funds.

2.3.3. Scenario Application

Users can verify their real names in an authoritative identity verification software such as CTID\(^{12}\). When they log in and register with other software, they only need to authorize the network certificate generated by the CTID platform, effectively preventing identity information leakage.
When a bank issues a loan, it will issue a "dyed" DECP, which is convenient for the relevant institutions to monitor the flow of funds. When the "dyed" DECP flows into the restricted industries, the system will give an alert and restrict or freeze the funds.

2.3.4. Feasibility Analysis

CTID is based on the legal ID card data of the Ministry of Public Security and adopts the national secret algorithm. The CTID platform desensitizes and de-identifies the identity information carried by the legal ID card, generates an irreversible data file, does not contain plaintext information, and is mapped to the legal ID card one, which can realize online identity authentication without revealing identity information.

Digital currency staining is also easier to achieve, as TEDA's issuance of USD stable coin USDT based on Bitcoin technology utilizes this technology. In issuing loans using DCEP, the loan currency can be "dyed" so that the loan flow does not have to be monitored all the time and only has to be verified as it flows into the restricted industry, reducing the cost of verification.

2.3.5. Potential Problems

At present, the number of institutions supporting CTID is relatively small, and the platform needs to promote the scope of application further. The "dyed" digital currency needs to be displayed in a specific client to show its label information, which is inconvenient to use.

3. Conclusion

This study proposes a blockchain-based solution to address the business pain points in trade settlement, delivery, and market supervision of futures exchanges. In trade settlement, blockchain technology can solve fairness and reliability, low settlement efficiency, high operation and maintenance costs and high settlement costs, enhance the processing speed of the trade settlement process, improve the transparency of the system and reduce operating costs. In terms of delivery, blockchain technology can reduce the cost of storing monitoring data in the storage process, improve the security of monitoring data, simplify the operation process between institutions and improve the efficiency of information circulation; in terms of regulation, blockchain technology can prevent credit funds from flowing into the futures market, protect customers' personal privacy and prevent leakage. Blockchain technology can provide new ideas for exchange business innovation and technical support for high-quality development of the futures market. It is recommended that domestic futures exchanges conduct research on blockchain technology to enhance market competitiveness.

References


https://uniswap.org/whitepaper.pdf


