



Research on blockchain based data trading methods and platforms

Zihan Wang^{1,a}, Jiqun Zhang^{*1,2,b}

¹School of Information Science and Engineering, Linyi University, 276000, China

²Shandong Linchuang Shugu Information Technology Co., Ltd, Linyi City, 276000, China

^a1731471923@qq.com, ^b1637636938@qq.com

Abstract. The emergence of blockchain technology provides a more secure, transparent and efficient way for data transaction. In this paper, based on the analysis of the basic principles and application scenarios of blockchain technology, the design scheme of blockchain-based data transaction method and platform is proposed. The scheme adopts smart contract to achieve automation of data transaction, adopts the storage form combining ethereum and ipfs to ensure the security and reliability of data storage, handles high-frequency and small amount transactions in the side chain and important high-value transactions in the main chain in order to improve the efficiency, and in order to protect the privacy of the data, homomorphic encryption can be introduced to ensure the privacy and security of the data in the process of transaction. Finally, the feasibility and effectiveness of the scheme are verified by implementing a prototype system of an Ethernet-based data transaction platform.

Keywords: blockchain; data transaction; smart contract; trust evaluation

1 Introduction

With the rapid development of the internet, data has become one of the most important resources in modern society. Typical applications of data trading include obtaining user data from internet companies, collecting environmental data from sensors and IoT devices, and acquiring transaction data from financial markets^[1-2]. However, traditional methods of data trading face many problems such as difficulty in ensuring data security, high transaction costs, and complex transaction processes. The emergence of blockchain technology provides a more secure, transparent, and efficient way of data trading.

Blockchain-based data trading methods mainly rely on the decentralized, tamper-proof, and traceable characteristics of blockchain technology to enhance data security and credibility^[3-4]. Moreover, blockchain-based data trading platforms possess features such as decentralization, autonomy, and openness that can improve data trading efficiency.

Homomorphic encryption techniques are classified into additive homomorphic encryption, multiplicative homomorphic encryption and full homomorphic encryption.

In this paper, full homomorphic encryption technique is used. Additive Homomorphism: If there exists an efficient algorithm \oplus , $E(x+y)=E(x) \oplus E(y)$ or $x+y=D(E(x) \oplus E(y))$ holds and does not leak x and y , then the encryption is said to be additive homomorphic encryption. Multiplicative homomorphism: an encryption is said to be multiplicative homomorphic if there exists an efficient algorithm for which $E(x \times y) = E(x)E(y)$ or $xy = D(E(x)E(y))$ holds and does not leak x and y . A fully homomorphic encryption is an encryption function that satisfies both the additive homomorphic and multiplicative homomorphic properties and can perform any number of addition and multiplication operations. Its formula is: $\text{Dec}(f(\text{En}(m1), \text{En}(m2), \dots, \text{En}(mk)))=f(m1, m2, \dots, mk)$, or written as: $f(\text{En}(m1), \text{En}(m2), \dots, \text{En}(mk))=\text{En}(f(m1, m2, \dots) =\text{En}(f(m1, \dots) \dots, mk))$, and if f is an arbitrary function, it is called a fully homomorphic encryption.

This article proposes a design scheme for blockchain-based data trading methods and platforms based on an analysis of the basic principles and application scenarios of blockchain technology. The scheme uses smart contracts to achieve automation of data trading and combines Ethereum and IPFS^[5-6] to ensure data storage security and reliability. Finally, the feasibility and effectiveness of the scheme are verified through the implementation of a prototype system of an Ethereum-based data trading platform.

2 Fundamentals of Blockchain Technology

2.1 Basic Principles of Blockchain Technology

The core of blockchain technology is distributed ledger technology. Blockchain organizes transaction records in chronological order into a chain structure, with each block containing multiple transaction records and the hash value of the previous block. Each node can participate in the creation and verification process of the blockchain, ensuring data consistency and security through consensus algorithms^[7].

2.2 Blockchain sidechain technology

High-frequency small transactions are processed on the sidechain in order to improve efficiency^[8]. Blockchain sidechain technology is a technology that interconnects different blockchains to enable asset transfer and value exchange^[9]. Sidechain technology was first proposed by Bitcoin for securely transferring money between the Bitcoin chain and other chains. Broadly speaking, sidechain technology applies to any blockchain system that meets the definition of a sidechain and has a main chain. Among the implementations of sidechain technology, there are two main ways: bi-directional wedging and joint wedging. Among them, bi-directional wedging refers to the mechanism of transferring assets on the main chain into or out of the side chains at a fixed or determined exchange rate, and its core mechanism is to lock a part of the assets on one chain and generate or unlock a part of the equivalent assets on the side chains.

3 Based on blockchain data trading method and platform

3.1 Design scheme

There are currently many data trading solutions, such as protecting data resources only through smart contracts, and decentralized data trading solutions that combine smart contracts with digital watermarks, but there are obvious problems in storage when the data exceeds 100MB. Therefore, I have designed a blockchain-based data trading method and platform using the storage format of Ethereum and IPFS, as shown in Figure 1:

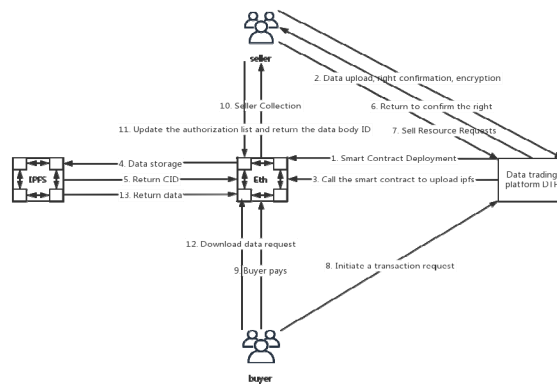


Fig. 1. Data transaction flowchart

(1) Data trading process.

The blockchain data trading process usually includes the following steps:

S1 Smart Contract Deployment: deploy smart contract into the public chain.

S2. data upload, rights confirmation, encryption: data owner prepares the data, data owner uploads the data to the chain, completing the transfer of data ownership. Data encryption adopts full homomorphic encryption technology: data includes sensitive data including transaction amount, identity information of both parties in the transaction, and so on. By encrypting the data with a public key, it can be ensured that only people holding the corresponding private key can decrypt and view the data.

S3. Invoke smart contract to upload the interstellar file system IPFS.

S4. Data storage: store the data to the interstellar file system IPFS.

S5. Return CID: data storage in the interstellar file system IPFS is completed to return the content identifier CID

S6. Return corroboration: when the content identifier CID is returned, the data is corroborated and the user ID in the transaction body TB is increased by the first user.

S7. The seller initiates a request to sell the resource. The data will be displayed in the data trading platform.

S8, S9. The buyer sends a transaction request to the seller, and after the seller agrees, the transaction is completed. The transaction confirmation session is done

automatically by the smart contract, which checks whether the subscriber has enough funds, and if the conditions are met, the funds are automatically transferred to the publisher's account

S10. the seller S account collects the money.

S11. update the authorisation list and return the data body ID: the buyer makes the payment and the seller's account receives the money both through the smart contract to complete the transfer. The transfer is completed updating the authorisation list with the user ID of the user who purchased the data.

S12. Download data request: the buyer payment is completed, you can data download, through the data trading platform, fill in the ID of the data you want to download, click on the download, the data trading platform will call the smart contract to obtain the interstellar file system IPFS data method, first of all, it will carry out the authorisation list user validation, check whether the user purchased the data or not, if user ID exists, then carry out the data download and return the private key.

S13. return data and verify: the buyer can use the purchased data. And verify the transaction result: homomorphic encryption allows computation in an encrypted state, so both parties in the transaction can verify that the transaction result is as expected without decrypting the data. This is achieved by using zero-knowledge proof techniques.

(2)Sidechain design

First design the sidechain. The design of the sidechain should take into account the compatibility with the Ethernet main chain, as well as the security and liquidity of the assets on the sidechain. At the same time, the design of the sidechain also needs to take into account factors such as development cost and maintenance cost.

Sidechain development: the development of the sidechain adopts the Ethernet smart contract language Solidity programming language. During the development process, attention is paid to the interaction logic between the sidechain and the main chain, as well as the security and privacy protection of the assets on the sidechain.

Sidechain Deployment: After the development of the sidechain is completed, it needs to be deployed into the Ethernet network. Register the sidechain on the Ethernet main chain, set up the governance mechanism of the sidechain, configure the asset transfer rules of the sidechain, and so on. At the same time, it is also necessary to conduct security tests and performance tests on the sidechain to ensure the stability and security of the sidechain.

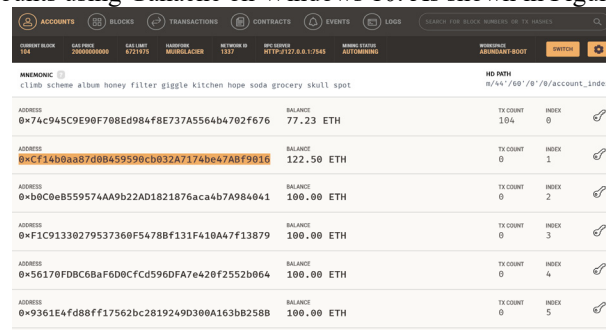
Sidechain and mainchain interconnection and intercommunication : Adopt two-way wedge mechanism to transfer assets on the mainchain to or from the sidechain at a fixed or determined exchange rate. In the bi-directional wedging mechanism, the transfer of assets between the main chain and the side chains needs to be realised through the process of locking and unlocking. Specifically, when a user wants to transfer an asset from the main chain to a side chain, he needs to lock the asset on the main chain and generate an equivalent asset on the side chain. Conversely, when a user wants to transfer an asset from a sidechain back to the main chain, he needs to lock the asset on the sidechain and unlock the equivalent asset on the main chain.

3.2 Implementation plan

The implementation plan of the blockchain-based data trading platform is as follows:

(1) Select blockchain platform.

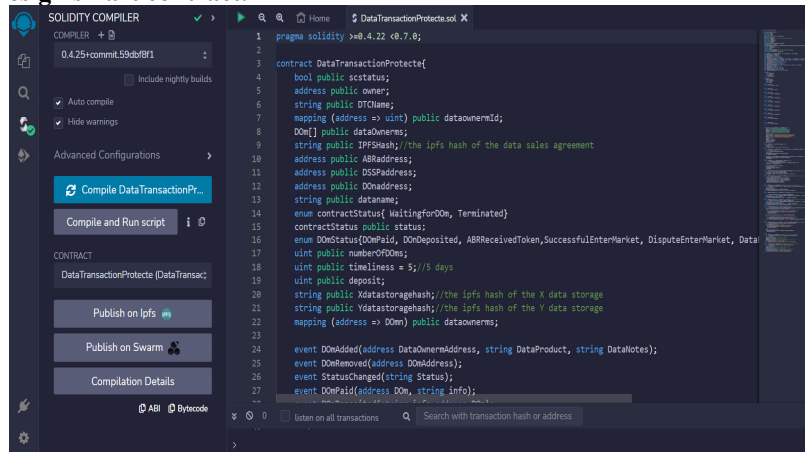
Choosing a suitable blockchain platform is the first step in implementing a blockchain-based data trading platform. This article uses the popular blockchain platforms Ethereum and IPFS. Ethereum experimental environment: This article simulates Ethereum accounts using Ganache on Windows 10. As shown in Figure 2.



ADDRESS	BALANCE	TX COUNT	INDEX
0x74c945c9E90F708Ed984f8E737A5564b4702f676	77.23 ETH	104	0
0xcfc14dbaa87d08459598cb32a7174bc47Abf9016	122.50 ETH	0	1
0xb0C0e8559574AA9b22AD1821876aca4b7A984041	100.00 ETH	0	2
0xF1C91330279537360F5478Bf131F410A47f13879	100.00 ETH	0	3
0x56178FDBC6BaF6D8cfcD596DFA7e420f2552b864	100.00 ETH	0	4
0x9361E4fd88ff17562bc2819249D300A163b8258B	100.00 ETH	0	5

Fig. 2. screenshot of Ethereum account

(2) Design smart contract.



```

1 pragma solidity >=0.4.22 <=0.7.8;
2
3 contract DataTransactionProtecte{
4
5     address public owner;
6     string public DTName;
7     mapping (address => uint) public dataownerId;
8     DOn[] public dataOwners;
9     string public IPFSHash; //the ipfs hash of the data sales agreement
10    address public ABRAddress;
11    address public DSSPAddress;
12    address public DOnAddress;
13    string public dtname;
14    enum contractStatus{ WaitingforDOn, Terminated}
15    contractStatus public status;
16    enum DOnStatus{DOnPaid, DOnDeposited, ABRReceivedToken, SuccessfulEnterMarket, DisputeEnterMarket, Data
17    uint public numberofDOns;
18    uint public timeliness = 5; //5 days
19    uint public deposit;
20    string public XdataStoragehash; //the ipfs hash of the X data storage
21    string public YdataStoragehash; //the ipfs hash of the Y data storage
22    mapping (address => DOnm) public dataowners;
23
24    event DOnAdded(address DataOwnerAddress, string DataProduct, string DataNotes);
25    event DOnRemoved(address DOnAddress);
26    event StatusChanged(string Status);
27    event DOnPaid(address DOn, string info);

```

Fig. 3. Remix IDE screenshot

Designing a smart contract is a key step in implementing a blockchain-based data trading platform. Smart contracts need to include functions such as data publishing, data subscription, and transaction confirmation, and introduce a trust evaluation mechanism. Build an Ethereum private chain in Remix IDE to test and verify the proposed smart contract. As shown in Figure 3.

4 Experimental results

To verify the effectiveness of the blockchain-based data trading method and platform, we have implemented a prototype system of an Ethereum-based data trading platform. The system uses smart contracts to automate data trading and introduces a trust evaluation mechanism to ensure the security and reliability of data trading. Through testing and deployment, we found that the system can operate stably and achieve automated data trading and trust evaluation.

5 Conclusion

This article proposes a design scheme for a blockchain-based data trading method and platform. The scheme uses smart contracts to automate data trading and introduces a trust evaluation mechanism to ensure the security and reliability of data trading. By implementing a prototype system of an Ethereum-based data trading platform, the feasibility and effectiveness of the scheme have been verified. In the future, we will further improve the system and apply it to actual data trading scenarios.

References

1. Gao X, Zhang W, Zhao B, Zhang J, Wang J, Gao Y. (2022). Product Authentication Technology Integrating Blockchain and Traceability Structure. *Electronics*(20), 3314-3314..
2. Zhao B, Zhang J, Cao W, Li B, Zhang W, Gao Y. (2023). A dynamic evaluation model of data price based on game theory. *Peer-to-Peer Networking and Applications*(5), 2073-2088..
3. Takegawa Naoki, Furuichi Noriyuki. (2023). Traceability Management System Using Blockchain Technology and Cost Estimation in the Metrology Field. *Sensors*(3), 1673-1673..
4. Zhang J, Li B, Zhao B (2024). Agricultural Internet of Things AI Big Data Platform Based on Blockchain. *Internet of Things Technology* (02), 121-122+126.
5. Zeng R, You J, Li Y, Zhou Y (2023). Design of Enhanced IPFS System Based on Information Center Network. *Network New Media Technology* (04), 58-68.
6. Wang L, Guo Y, Zhu Y, Duan Z (2022). Monitoring Information Privacy Protection Mechanism Based on Blockchain and IPFS. *Electronic Design Engineering* (11), 178-182+188.
7. Zhai S, Lian J, Yang R and Liu F (2023). Practical Byzantine fault-tolerant consensus algorithm based on Raft grouping. *Computer application research* (11), 3218-3224+3234.
8. Singh, A., Click, K., Parizi, R. M., Zhang, Q., Dehghantanha, A., & Choo, K. K. R. (2020). Sidechain technologies in blockchain networks: An examination and state-of-the-art review. *Journal of Network and Computer Applications*, 149, 102471.
9. Rahman, A., Hossain, M. S., Rahman, Z., & Shezan, S. K. A. (2019). Performance enhancement of the internet of things with the integrated blockchain technology using RSK sidechain. *International Journal of Advanced Technology and Engineering Exploration*, 6(61), 257-266.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

