RESEARCH

A Blockchain-Based Spatial Data Trading Framework

Hui Liu[1,2]
, WeiPeng Tai[2], Yaofei Wang[1] and Shenling Wang[1*]

*Correspondence: slwang@bnu.edu.cn
[1]School of Artificial Intelligence, Beijing Normal University, Beijing, China
Full list of author information is available at the end of the article

Abstract

With the increasing utilization of space related data, the demand for spatial big data sharing and trading is growing rapidly, which promotes the emergence of spatial data market. However, in conventional data markets, both data buyers and data sellers have to use a centralized trading platform which might be dishonest. Blockchain is a decentralized distributed data storage technology, which uses the traceability and unforgeability to confirm and record each transaction, can solve the disadvantages of the centralized data market, however, it also introduces the problems of security and privacy.

To address this issue,in this paper,we propose a blockchain-based spatial data trading framework with Trusted Execution Environment to provide a trusted decentralized platform, including data storage, data query, data pricing and security computing. Based on this framework, a spatial data trading demonstration system was implemented and its feasibility and security were verified.

Keywords: spatial data; data trading; data pricing; Blockchain

Introduction

With the increasing popularity of all kinds of sensors and the wide application of mobile positioning technology, the amount of spatial data is increasing rapidly. Spatial data has become a key asset in our economy, the utilization of spatial data can bring huge economic benefits or help us make better decision. In order to ensure the normal circulation and use of data, many emerging institutions about spatial data sharing and trading have emerged in recent years. In addition to the traditional way of data circulation, there is also a big data trading market, which facilitates data transactions by matching data demand with data sources.

In a conventional data market [1–4], data seller sends the data to a centralized trading platform. Although the data trading platform accelerates the sharing and circulation of data, there are still many problems in the data trading platform at present:

1)The dishonest data buyer may resell the data seller's data to others after obtaining the data seller's data, thus damaging the data seller's interests. At present, the data circulating on the data trading platform is the source data without data analysis, and the data has the feature of "read it and have it". That is to say, malicious data buyers can cache the source data and resell them to others at a lower price than the data seller after purchasing the data.

2)The centralized trading platform may be dishonest who may cache and resell the source data without the permission of the data seller, thus damaging the interests of both parties to the transaction.

3)When data trading platform is a centralized system with low fault tolerance for faults or attacks, once a fault occurs or is attacked by an attacker, the entire data trading platform may be paralyzed, which will affect the data transaction between the data buyer and the data seller, and even cause the leakage or loss of key data of the platform.

In addition, the centralized trading platform lacks effective information communication channel between data buyer and data seller, which leads to low efficiency of data transaction [5].

In order to avoid the disadvantages in centralized data market, such as data security and privacy, data copyright protection and sharing and circulation performance bottlenecks, decentralized data market was born. Decentralized data market architecture can get rid of single point of failure and single point of performance bottleneck, and improve the transparency and credibility of data transactions. However, due to the lack of centralized management in decentralized data market, its system design and security assurance will be more difficult than centralized data market. For example, double payment has always been the difficulty of distributed system [6, 7].

Blockchain is a distributed public ledger first introduced by Nakamoto in 2008 [8]. It maintains a continuously growing list of ordered records called blocks. Each block in the chain is linked to the previous block through a cryptographic hash. All nodes in the network share the same copy of digital ledger. Information stored in the blockchain is open to everyone, making the actions of nodes transparent.

The introduction of blockchain into the data market system will enable data sellers to enter into transactions with the data buyers directly without relying on any third party, so that sellers can maintain the ownership of data and ensure the openness and transparency of the transaction process, can solve the disadvantages of the centralized data market, however, it also introduces the problems of security and privacy [9–12], as explained below:

1)Data files are stored safely. In the scenario of data trading, the data files to be traded by both parties need to be properly stored. First of all, data files cannot be stored in the blockchain. The design of the blockchain system is only suitable for storing transaction data with a small amount of data, but not suitable for storing data files with a large amount of data. Secondly, the data file stored procedure cannot disclose identity information. Finally, it is necessary to ensure that the data buyer can easily obtain the data, and the buyer and the seller can not identify the real identity of the other party.

2)Privacy protection. Based on the business requirements of blockchain and data transaction, it is necessary to research and design privacy protection scheme in data transaction process, to protect the user's real identity from being disclosed and ensure the security of transaction data under the condition of ensuring the normal operation of data transaction.

To address this issue, we propose a blockchain based spatial data trading framework which takes advantages of the blockchain to build a decentralization platform

for data trading, including data storage, data query, data pricing and security computing.

To tackle the first challenge, we use IPFS (InterPlanetary File System) to store data files, which is a distributed file storage system. When a file is uploaded to IPFS, it is available to all peers in the IPFS network. the user will receive a hash index, which will allow the user to retrieve the file later. This index will replace the data stored in the smart contract, saving the burden of the entire system.

To address the second challenge, we adopt smart contract to realize the data transaction, and the combination of cryptography technology and Ethereum account mechanism is used to solve the privacy protection and data security problems in the transaction.

In our design, data buyers and data sellers conduct transactions directly on the blockchain, which avoids risks caused by centralized trading platforms. All payment records and reviews generated by data buyers are faithfully recorded in the blockchain through consensus protocol, and can be protected securely with Trusted Execution Environment. The rest of this paper is organized as follows: In Section 1, we introduce the background and related work. In Section 2, we design the framework of spatial data trading based on blockchain. In Section 3-4, we verify feasibility and security of a spatial data trading system. At last, we summarize our results and make some concluding remarks.

1 Background Knowledge

Due to its decentralized immutable and traceable characteristics, blockchain technology is used in data trading market in recent years, which has attracted great attention of the industry. Some of these companies directly sell their collected data sets, while others collect personal data from the public and sell it to individual users. There are also some domestic examples of using blockchain technology to build data market. For example, Shanghai Data Trading Center [13] uses alliance chain to store transaction related information in blockchain nodes to ensure data transaction security, efficiency and credibility.

Zyskind [14]used blockchain to protect the privacy of personal data, transforming the blockchain into an automatic access control manager that does not rely on trusted third parties to clarify the ownership of data and ensure that users control their data. However, this work only discusses the storage and sharing of data. Crowdbc [15] is a group intelligence perception system constructed by blockchain. The author focuses on the characteristics and processing methods of image data in transaction. Baig [16] constructed a data market based on blockchain, and introduced a trusted intermediary in the transaction between the buyer and the seller. Although this makes the transaction between the buyer and the seller easier, it also reduces the security of the system a lot. Dai proposed SDTE [17], a blockchain-based data trading ecosystem. In SDTE, buyers of data cannot directly access the original data they purchased, and can only obtain the analysis results of the data, which is generated from Intel SGX (Software Guard Extensions). However, if there are too many malicious data sellers in a transaction, honest data sellers will not be able to get reasonable compensation.

Spatial data in this paper includes [18]: remote sensing, mapping and other raw data, such as low-resolution satellite images, medium resolution satellite images,

high-resolution satellite images, sub meter high-resolution satellite images, radar data, aerial photogrammetry data, series scale vector data, terrain data, and other types of original spatial information data. As shown in Figure 1, after obtaining spatial data through various devices such as mobile phones and satellites, the data owners upload them to the cloud storage platform through network, and then sell them to the data buyers through data trading platform.

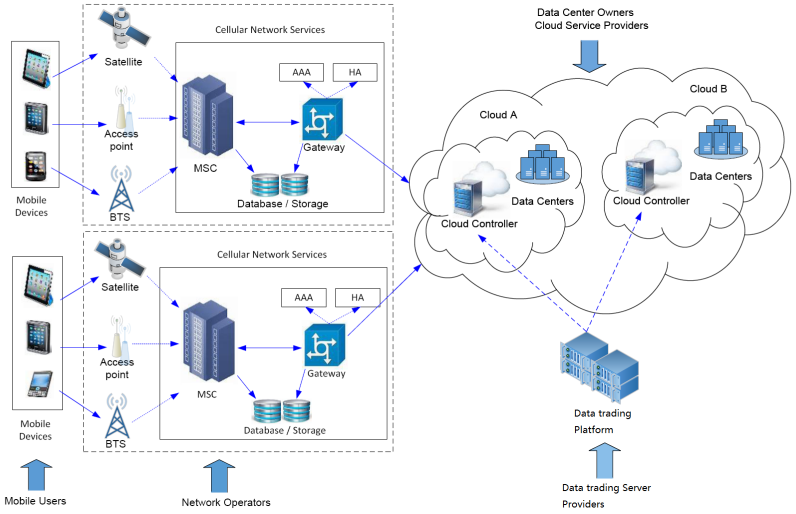

Figure 1: Spatial data trading system

The spatial data trading system based on blockchain designed in this paper consists of three main components: a smart contract in Ethereum blockchain, client held by system participants and a point-to-point data transmission network. When a data buyer needs some specific data to calculate a specific task, he will use the data query module and inform the smart contract. The whole system locates some qualified data through the way of security calculation. After the interaction between the data buyer and the data seller, the data pricing module will determine the sale data and its price. After the payment is completed, the system runs the buyer's calculation task in the way of security calculation, and returns the results to the buyer, and the transaction is completed.

1.1 Data query

Data buyers usually don't need all the data of the seller, but care about the specific data. Buyers can organize their own data requirements into a logical expression or a mathematical function and store them in the blockchain for the seller to query and judge [19, 20].

The query conditions of these data are generally relatively simple, so it is not appropriate to upload the buyer's data query requirements directly to the blockchain, which obviously exposes the privacy of buyers and sellers. According to the form of data query, it is easy for attackers to infer the buyer's data requirements and obtain the privacy of the buyer and the seller. If a location of interest to the buyer is disclosed, the attacker may infer the buyer's range of activities, and the device

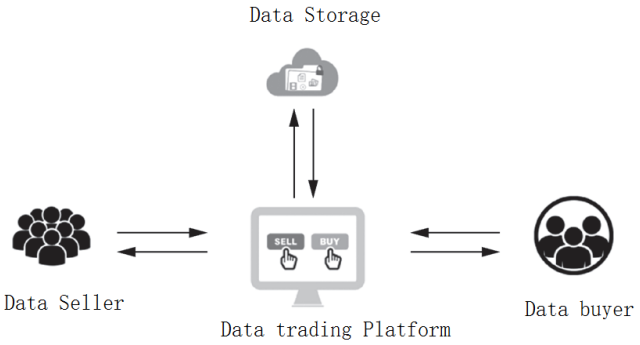

Figure 2: Data trading platform

held by the seller close to the location is also exposed. Therefore, in order to protect the privacy of system participants, we should query the target data while hiding the query conditions. The most intuitive solution is function encryption, that is, the buyer with decryption key can obtain the data query function value of ciphertext data , but will not obtain any information about original text.

1.2 Data storage

The mainstream public blockchain has restrictions on the number and space of transactions in the block. The limit is the size of the block (bitcoin) or the upper limit of "natural gas" consumed in the block (Ethereum). For the data trading market, it is not feasible to store massive data directly on the blockchain. Recently emerged a distributed data storage InterPlanetary File system (IPFS) is introduced for storing the shared data in various other domains like healthcare, cloud computing, IoT, and agriculture.

IPFS [21–23]is a peer to peer, content-addressable, distributed file storage system, using a swarm of computers connected. When a file is uploaded to IPFS, it is available to all peers in the IPFS network. The uploaded file is divided into chunks, that are assigned a unique cryptographic hash. Thus, data added to IPFS is addressed by using this unique cryptographic hash, which makes it content addressable. It uses distributed hash tables (DHTs) to find locations of files. Thus, storing traded data in IPFS and the hashes returned by IPFS are stored in blocks, which reduces the huge cost of storage space. In summary, IPFS provides high throughput with secure storage model that supports concurrent access of data with high storage capacity.

The cloud storage service of the spatial big data trading platform is mainly to establish a storage space station, which uses computer, Internet, Internet of things and other technologies to carry out daily storage management on the products and services traded by the platform and various information generated in the transaction process, and can quickly and accurately complete the statistical summary of product and service transaction information. Taking the advantages of cloud storage service, such as rapid retrieval, convenient search, high reliability, large amount of storage and good confidentiality, a large number of data can be safely saved [24].

Although it is impractical to store the complete data in the blockchain, the data digest bound with specific data can be stored in the blockchain, and the data can be

stored in IPFS. When the data is successfully stored in IPFS, the user will receive a hash index, which will allow the user to retrieve the file later. This index will replace the data stored in the smart contract, saving the burden of the entire system.

1.3 Data pricing

In the data market, the design of data selling form and the setting of price has always been an active research field. In this paper, we consider the design of pricing mechanism in the environment of game theory. Each data holder has a private valuation for their data, that is, the loss of privacy of the data seller is leaked; the data buyer also has a valuation for the data he will buy, that is, the value of the data to the buyer. Bidders may choose to dishonestly report their valuation of a piece of data. The solution in game theory is to design incentive compatible mechanism so that each bidder can get the highest return when reporting its real valuation. The fact that bidders report their true valuations makes it much easier to design pricing mechanisms.

As a commodity, data has some unique properties [25, 26] , which make data pricing need to consider some additional issues. First, the marginal cost of data is extremely low, or there is no marginal cost at all. Marginal cost refers to the cost of making a copy of a good after it is produced. The marginal cost of data is basically zero, so that once the data buyer obtains the data of the data seller, he may resell the data. Second, the value of data is not necessarily related to the amount of data. For example, for a person who needs remote sensing images, a pile of face images is of little value. The third is the quantification of data value. The value of data is difficult to quantify, and it is difficult for data sellers to estimate the value of data. At the same time, valuations vary greatly among different buyers.

According to the characteristics of data, the data trading mode in the data market has also changed. The traditional data market will directly trade the user's data, and dishonest buyers can resell their purchased data sets without the seller's knowledge, so as to obtain benefits. Many studies have found that most data consumers only need some statistical results or advanced features behind a large amount of data, such as calculating the average value of data sets, or training data for machine learning models, rather than the data itself. As a result, data markets can collect data from data sellers and then serve the computing tasks in the hands of data consumers. The buyer provides a specific task, whose input is the right to use multiple copies of data purchased, while the output is the result the buyer wants. In this way, the data itself is isolated from the data consumer.

Although the value of the data itself is difficult to quantify, the seller's task calculation results are easy to quantify. Since buyers often need data from multiple sellers, it is necessary to distinguish the value of each data in a transaction. When calculating the value of data, Shapley value can be used to calculate the contribution of single data [27] . In game theory, calculating Shapley value is a solution to distribute benefits and costs equally to multiple participants. The computation complexity of Shapley value increases exponentially with the increase of data quantity, so approximate algorithm is often used in practical application.

1.4 Security computing

Blockchain is an open, transparent and decentralized data storage technology. All information entering the blockchain system is open, and the execution of all transactions or scripts is transparent. At the same time, the computing power of the blockchain smart contract is very weak. Due to the limitation of block size and gas, the calculation of a smart contract is very small, but the cost is high. Therefore, it is not safe to run the trading transactions issued by the buyer directly in the smart contract. Similarly, such problems also exist in the process of data query and data pricing. Bitcoin, Ethereum and other blockchain public chain nodes are not trusted with each other, but also completely open and transparent, which makes the privacy protection work produce new problems.

Trusted hardware, such as trusted execution environment (TEE) [28–30], is a common method to implement secure computing. TEE ensures that the code and data loaded in it are protected in terms of confidentiality and integrity. Assuming that some users have some TEE hardware, they are considered as secure users. The seller will send their data to the TEE equipment of the secure user, and the calculation task of the buyer will be calculated in the TEE and the result will be returned to the buyer in a safe way. Only trusted applications running in TEE can access the full functionality of the device's main processor, peripherals, and memory. Hardware isolation protects data and computing content from user installed applications running on the main operating system. The typical hardware technologies supporting tee implementation are arm TrustZone and Intel SGX software guard Extensions.

Intel Software Guard Extensions (SGX) [31] provides a widely used TEE implementation for general-purpose computation, which is known as enclaves in SGX. Code running inside a enclaves has a protected address space. When data from a enclave moves off the processor to memory, it is transparently encrypted with keys only available to the processor. Thus the operating system, hypervisor and other users cannot access the enclaves memory. In the enclave, the code and data are measured at the startup stage and the measurement is signed into an attestation report based on a hardware-based root of trust. The report can be verified to show the unmodified enclave code logical, by which users can confirm the security of enclave and provision the secret into the enclave at runtime, which is called remote attestation protocol.

In this paper, we use Intel SGX as the exemplary implementation to build a trusted exchange by using Trusted Execution Environment, assisting in the fair payment of the transactions.

2 The Proposed Framework

We have implemented a spatial data trading system based on Ethereum private chain, including system participants holding desktop application clients, smart contracts in Ethereum network and data transmission network. The desktop client is written by JavaScript, Ethereum smart contract is written by solidness, and the JS interface of IPFS is directly used for data transmission.

We simplify the system into one buyer and multiple potential sellers to trade. One buyer only needs one data. The pricing mechanism adopts the second price auction, that is, the transaction data adopts the lowest bid data of the seller, and the data is

paid at the second lowest price. The buyer's computing task is set to be simple, and it can be ensured by homomorphic encryption or secure multi-party computing.

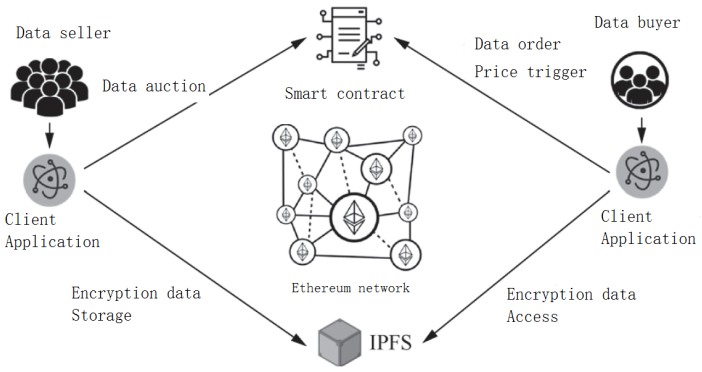

Figure 3: Data trading framework based on blockchain

The data transaction process is shown in Figure 3 The data seller adds a new data information in the smart contract, and the data buyer adds an order containing data requirements. The seller gives a quotation after matching the legal data according to the conditions in the order. The system will run the pricing mechanism and calculate the data for sale. The data trading platform will calculate the buyer's task and deliver the data through the security calculation method.

To describe how the framework works, we introduce the main workflow of the system.

Step1: Regist data. To buy and sell data in the data market, the user must first register an Ethereum account, and the client also contains a simple Ethereum account management function. At the same time, the user also needs to register an account in the smart contract. For example, the user can register an account of a sensor device in the smart contract, which needs to disclose the type, model and other information of the sensor device.

Step2: Add data. After generating some data that he wants to sell, the data seller can encrypt and upload the data to IPFS, and register the data in the smart contract account, including the storage address, hash value and registration time of the data. Data buyers are encouraged to set data registration time requirements when adding data orders to purchase data. Only data sellers who meet the data registration time requirements are eligible to bid for the order, so as to improve the timeliness and reliability of data.

Step3: Issue orders. If a data buyer wants to buy a right to use specific data in the market, he will add an order to the smart contract. The order contains the buyer's demand for data (including data type, data selection function, data price limit, data quantity limit, etc.) and the calculation task for the buyer to use the data.

Step4: The data seller provides a hash of their bid. Data sellers choose one or more pieces of data that meet the needs of data buyers and set a package price.

Step5:The Data Buyer notifies the smart contract to obtain the real bid of the market data seller. The Data Buyer notifies smart contract to stop accepting users

from participating in the transaction, and begins to accept users who have participated in the transaction to disclose their bids.

Step6:Data sellers announce real bids. The data seller publishes its bid, which needs to match the previous hash value.

Step7:Pricing mechanism. The classic Vickrey-Clarke-groves auction mechanism is used for data selection and price determination. The VCG auction mechanism guarantees authenticity, so each bidder has an incentive to make a true evaluation of his personal data.

Step8:Deliver data. The system will use homomorphic encryption to calculate the buyer's calculation task, and then send the encrypted results to the data buyer to complete the order.

3 System analysis

3.1 privacy analysis

The identity privacy and data privacy of system participants are protected in the system. Identity privacy is based on the anonymity ability of blockchain, while data privacy is fully protected. Data encryption, data selection mechanism and secure computing make attackers unable to obtain any additional information of data from the execution of transactions.

3.2 pricing analysis

Since data pricing is implemented on the Ethereum blockchain through smart contracts, its computational cost cannot be ignored. In order to evaluate the data pricing cost of the system, the data pricing based on VCG auction is used to test the gas consumption when a large number of sellers bid in the transaction. Figure 4 shows the relationship between the gas consumption of VCG data pricing and the number of bids received for data orders. We find that when a large number of data sellers bid for the same data order, the data pricing cost will be very high. If we want to realize the data market based on Ethereum blockchain, the high cost of data pricing will become the obstacle of system application. Therefore, in the follow-up study, reducing the cost of data pricing is one of the future research directions.

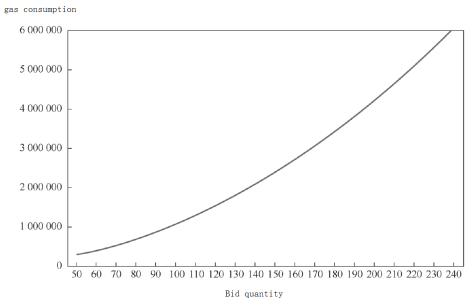

Figure 4: Relationship between gas consumption and bid quantity

4 Experimental Methods

We have implemented a spatial data trading system based on Ethereum private chain, smart contracts in Ethereum network and data transmission network. All the

tests of this system are completed on PC with 4 vcores(3 GHz Intel Xeonr Platinum 8124M) and 8 GB RAM. The desktop client is written by JavaScript, Ethereum smart contract is written by solidness, and the JS interface of IPFS is directly used for data transmission. The online transaction module of data transaction system is implemented in Python language.

This paper mainly tests the system throughput, storage space occupation and fault tolerance. Among them, for the system throughput, we mainly test the amount of data that can be processed per unit time under the condition of different number of nodes and different data through concurrency test; for the storage space, we mainly test the disk space required for data link under different number of nodes; for the fault tolerance performance, we compare the impact of node failure on the overall throughput in different modes.

In Consortium BlockChain such as fabric, node throughput is limited by communication delay, transaction verification time and hash operation time. In a system with N nodes and an average block of T transactions, assuming the node communication delay t_c, transaction verification time t_v, and one hash operation time t_h, the throughput of the whole system is shown in equation:

$TPS = \frac{T}{N^2 \times t_c + T \times t_v + 2 \times T \times t_h}$.

In order to test the storage requirement for packaging transactions throughout the system, this paper compares the storage reduction after packaging the chain by constructing the same number of transaction requests. In an N-node blockchain system, the number of included transactions is T, assuming that the average space occupied by each transaction is s_t, and the space occupied by a hash result is s_h. then we can estimate the disk space occupied as $S = N \times T \times (S_t + S_h)$.

5 Experimental Evaluation

In order to test the running speed of the system, we list the running time tests of sub key generation, data encryption and Merkel tree generation. The generation of subkey and Merkel tree are based on binary tree, so their running time is closely related to the depth of the tree. We use $L = \lceil \log_2 n \rceil + 1$ to calculate the depth of the tree, where n represents the number of transaction data. The test results are shown in Figure 5.

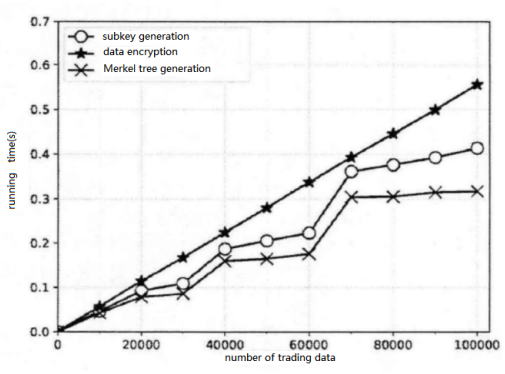

Figure 5: running time tests

With the increase of the number of transaction data n, the depth L of the tree increases, and the generation time of the final sub key and Merkel tree also increases. The test results in Figure 5 show that when the number of transaction data is 60000, the depth of the sub key generation tree and Merkel tree is 17, while when the number of transaction data is 70000, the depth of the tree reaches 18, and the increase of the depth of the tree increases the running time of the sub key generation and Merkel tree generation by about $0.14s$.

With the increase of the number of nodes, transaction throughput of the system increases significantly, which is higher than that of fabric system. The transaction throughput of the traditional blockchain platform is relatively stable, while the transaction throughput of the blockchain system described in this paper can increase rapidly with the increase of the number of nodes. The blockchain system described in this paper can effectively improve the transaction throughput, as shown in Figure.6.

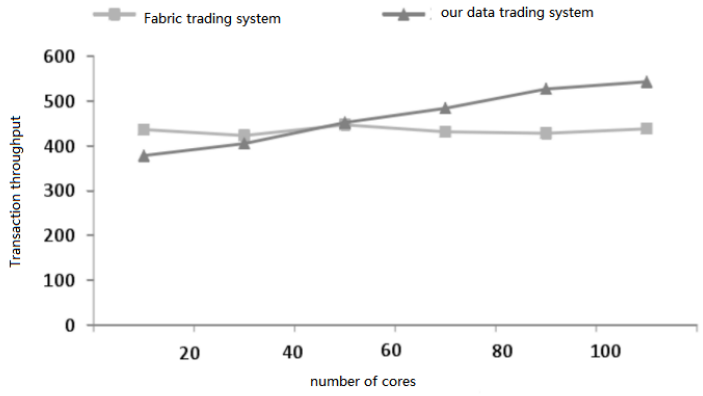

Figure 6: Transaction throughput tests

In order to test the storage requirement for packaging transactions throughout the system, this paper compares the storage reduction after packaging the chain by constructing the same number of transaction requests.

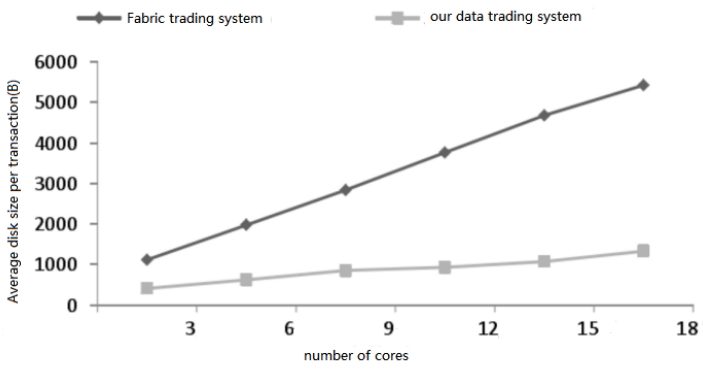

Figure 7: storage tests

As shown in Figure. 7, when the number of nodes in a traditional block chain increases, the total space occupied by transactions increases almost linearly. However, the block chain system described in this paper increases disk space slowly as nodes increase. It can greatly reduce storage costs when dealing with large amounts of data chained.

By comparing the success rate of malicious attack on the distributed deployment of traditional centralized system, traditional federation chain system and the system under different ratio of malicious nodes, this paper uses 120 block chain nodes for convenience. As shown in Figure.8, in the centralized system of traditional distributed deployment, as long as there are malicious nodes, the attack success rate is 100%. In the traditional PBFT based blockchain system [32, 33], if the number of malicious nodes is less than 1/3, fault tolerance can be achieved smoothly, but if it exceeds 1/3, it will be affected. This system can tolerate more node failures and reduce the risk of transaction blocking.

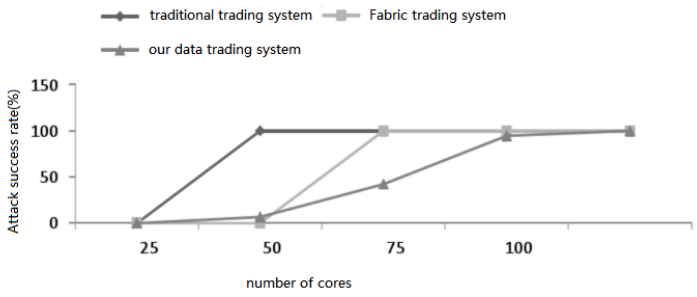

Figure 8: Fault tolerance tests

6 Results and Discussion

The final test results show that the system described in this paper has better throughput, less storage space occupation and better fault tolerance, and can adapt to the high frequency and real-time requirements of data trading.

"Scalability Triple Difficulty" refers to the unavoidable contradiction among scalability [34], decentralization and security of block chain systems. The system is a completely decentralized system and does not rely on any trusted third party, so scalability and security will be more challenging. In order to ensure security, the system proposed in this paper sacrifices scalability. In the future deployment of the data trading system, we will further explore the trade-off between scalability, decentralization and security.

7 Conclusion

In this paper, we propose a blockchain based spatial data trading framework which takes advantages of the blockchain to build a decentralization platform.

The platform provides data and platform interface, with petabyte level remote sensing data storage and processing capabilities; without prior installation, users can obtain the integrated services of remote sensing data, information, software and

computing resources through the cloud service terminal; users can use the space information infrastructure anytime and anywhere, without purchasing data, software and expensive computer equipment in order to use high resolution remote sensing information conveniently and economically, it can greatly reduce the threshold of remote sensing in terms of cost and maintenance.

Funding

This work was supported by National Natural Science Foundation of China under Grants 61772080 and the Fundamental Research Funds for the Central Universities under Grants 2020NTST32.

Abbreviations

IPFS: InterPlanetary File System
SDTE: Secure Blockchain-Based Data Trading Ecosystem
SGX: Software Guard Extensions
DHTs: distributed hash tables
TEE: trusted execution environment
VCG: Vickrey-Clarke-groves
PBFT: Practical Byzantine Fault Tolerance

Availability of data and materials

Data sharing is not suitable for this paper, because a lot of data in this paper is personal privacy data, which needs relevant legal protection.

Competing interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Authors' contributions

Liu Hui carried out the design of the trading system in this paper drafted the manuscript. WeiPeng Tai colloected the data, Yaofei Wang participated in the design of smart contract, Shenling Wang carried out the experimental evaluation and performed the statistical analysis. All authors read and approved the final manuscript.

Author details
[1]School of Artificial Intelligence, Beijing Normal University, Beijing, China. [2]School of Computer Science and Technology, An Hui University of Technology, Maanshan, China.

References

1. Misura, K., Zagar, M.: Data marketplace for internet of things. In: 2016 International Conference on Smart Systems and Technologies (SST) (2016)
2. Zhao, D., Ye, C., Zhang, B.: Data marketplace and its values in data trading. Library and Information Service (2017)
3. Pang, J.Z.F., Fu, H., Lee, W.I., Wierman, A.: The efficiency of open access in platforms for networked cournot markets. In: IEEE Infocom -ieee Conference on Computer Communications (2017)
4. Ramachandran, G.S., Radhakrishnan, R., Krishnamachari, B.: Towards a decentralized data marketplace for smart cities. In: 2018 IEEE International Smart Cities Conference (ISC2) (2019)
5. Nguyen, D.D., Ali, M.I.: Enabling on-demand decentralized iot collectability marketplace using blockchain and crowdsensing. In: Global IoT Summit (2019)

6. Su, G., Yang, W., Luo, Z., Zhang, Y., Zhu, Y.: Bdtf: A blockchain-based data trading framework with trusted execution environment (2020)
7. Sadiq, A., Javaid, N., Omaji, S., Khalid, A., Imran, M.: Efficient data trading and storage in internet of vehicles using consortium blockchain. In: 16th International Wireless Communications and Mobile Computing Conference (IWCMC), 2020 (2020)
8. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. Online at `https://bitco.in/pdf/bitcoin.pdf` (2008)
9. Zheng, X., Mukkamala, R.R., Vatrapu, R., Ordieres-Mere, J.: Blockchain-based personal health data sharing system using cloud storage, pp. 1–6 (2018)
10. Ruinian, L., Tianyi, S., Bo, M., Hong, L., Xiuzhen, C., Limin, S.: Blockchain for large-scale internet of things data storage and protection. IEEE Transactions on Services Computing, 1–1 (2018)
11. Jiang, T., Fang, H., Wang, H.: Blockchain-based internet of vehicles: Distributed network architecture and performance analysis. IEEE Internet of Things Journal **6**, 4640–4649 (2019)
12. Liu, X., Huang, H., Xiao, F., Ma, Z.: A blockchain-based trust management with conditional privacy-preserving announcement scheme for vanets. IEEE Internet of Things Journal **7**(5), 4101–4112 (2020)
13. WANG, J., ZHENG, Z., WU, F., CHEN, G.: Blockchain based data marketplace. Big Data **6**(03), 25–39 (2020)
14. Zyskind, G., Zekrifa, D.M.S., Alex, P., Nathan, O.: Decentralizing privacy: Using blockchain to protect personal data. In: IEEE Security and Privacy Workshops (2015)
15. Li, M., Weng, J., Yang, A., Lu, W., Zhang, Y., Hou, L., Jia-Nan, L., Xiang, Y., Deng, R.: Crowdbc: A blockchain-based decentralized framework for crowdsourcing. IEEE Transactions on Parallel and Distributed Systems, 1–1 (2018)
16. Baig, F., Wang, F.: Blockchain enabled distributed data management - a vision. In: 2019 IEEE 35th International Conference on Data Engineering Workshops (ICDEW) (2019)
17. Dai, W., Dai, C., Choo, K.K.R., Cui, C., Zou, D., Jin, H.: Sdte: A secure blockchain-based data trading ecosystem. IEEE transactions on information forensics and security **15**, 725–737 (2020)
18. Anselin, L., Syabri, I., Kho, Y.: Geoda: An introduction to spatial data analysis. Geographical Analysis (2006)
19. Li, R., Liu, A.X., Wang, A.L., Bruhadeshwar, B.: Fast range query processing with strong privacy protection for cloud computing. In: Proc. the VLDB Endowment (2014)
20. Kang, J., Yu, R., Huang, X., Wu, M., Maharjan, S., Xie, S., Zhang, Y.: Blockchain for secure and efficient data sharing in vehicular edge computing and networks. IEEE Internet of Things Journal **6**(3), 4660–4670 (2019)
21. Chen, Y., Li, H., Li, K., Zhang, J.: An improved p2p file system scheme based on ipfs and blockchain. In: 2017 IEEE International Conference on Big Data (Big Data) (2017)
22. Vimal, S., Srivatsa, S.K.: A new cluster p2p file sharing system based on ipfs and blockchain technology. Journal of Ambient Intelligence and Humanized Computing (2) (2019)
23. Wu, X., Han, Y., Zhang, M., Zhu, S.: Secure Personal Health Records Sharing Based on Blockchain and IPFS, (2020)
24. Naz, M., Al-Zahrani, F.A., Khalid, R., Javaid, N., Qamar, A.M., Afzal, M.K., Shafiq, M.: A secure data sharing platform using blockchain and interplanetary file system. Sustainability **11** (2019)
25. Sen, S., Joe-Wong, C., Ha, S., Chiang, M.: Pricing data: A look at past proposals, current plans, and future trends. Acm Computing Surveys (2012)
26. Dziembowski, S., Eckey, L., Faust, S.: Fairswap: How to fairly exchange digital goods. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018, pp. 967–984. ACM, ??? (2018). doi:10.1145/3243734.3243857. https://doi.org/10.1145/3243734.3243857
27. Shi, W., Wu, C., Li, Z.: A shapley-value mechanism for bandwidth on demand between datacenters. IEEE Transactions on Cloud Computing **6**(1), 19–32 (2018)
28. Eltayieb, N., Elhabob, R., Hassan, A., Li, F.: A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud. Journal of Systems Architecture **102**, 101653 (2019)
29. Feng, Q., He, D., Zeadally, S., Liang, K.: Bpas: Blockchain-assisted privacy-preserving authentication system for vehicular ad-hoc networks. IEEE Transactions on Industrial Informatics **PP**(99), 1–1 (2019)
30. Jeong, B.G., Youn, T.Y., Jho, N.S., Shin, S.U.: Blockchain-based data sharing and trading model for the connected car. Sensors **20**(11), 3141 (2020)
31. Hoekstra, M., Lal, R., Pappachan, P., Phegade, V., Cuvillo, J.D.: Using innovative instructions to create trustworthy software solutions. In: Proceedings of the 2nd International Workshop on Hardware and Architectural Support for Security and Privacy (2013)
32. Tang, J., Cui, Y., Li, Q., Ren, K., Liu, J., Buyya, R.: Ensuring Security and Privacy Preservation for Cloud Data Services. ACM Computing Surveys **49**(13) (2016)
33. Wang, G., Nixon, M.: Randchain: Practical scalable decentralized randomness attested by blockchain. In: 2020 IEEE International Conference on Blockchain (Blockchain) (2020). IEEE
34. Kraft, D.: Difficulty control for blockchain-based consensus systems. Peer-to-Peer Networking and Applications (2016)

Figure

Figure 1: Spatial data trading system

Figure 2: data trading platform

Figure 3: data trading framework based on blockchain

Figure 4: Relationship between gas consumption and bid quantity

Figure 5: running time tests

Figure 6: Transaction throughput tests

Figure 7: storage tests

Figure 8: Fault tolerance tests