Implementing an Asset Trading System Based on Blockchain and Game Theory

Haihui Huang[1], Jing Cai[1], Shaoci Xie[2]
[1]School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing, China
[2]School of Software Engineering, Chongqing University of Posts and Telecommunications, Chongqing, China
Emails: huanghh@cqupt.edu.cn, s170131064@stu.cqupt.edu.cn, xiesc@cqupt.edu.cn

Abstract—With the development of the Internet and e-commerce, an asset trading system has become more and more complicated. There are security obstacles such as the untrustworthy third-party service in the centralized management system of asset transactions. Thanks to the advanced features of openness, immutability and decentralization of blockchain technology. It is expected to solve the trust problem between buyers and sellers. Based on the Hyperledger Fabric platform, we first present an asset trading system that implements smart contracts for asset release and asset trading. Moreover, we evaluate the performance of the system using Hyperledger Caliper and test functions of system by Postman. To address issues of matching buyers and sellers, a matching model based on game theory is proposed. In this process, the user's reputation value and buyer's bid are used to determine the seller's matchable range, which aims to find the optimal equilibrium solution for buying and selling profit. Our experimental result proves that this system's average latency is less than 0.27S and the event response success rate is 1 basically, when the maximum throughput of the system is not exceeded.

Keywords-blockchain; assert trading; Hyperledger Fabric; smart contract; e-Auction

I. INTRODUCTION

With the rapid development of Internet technology, asset information and product information of enterprises or individuals are gradually becoming digital. E-commerce, remote transactions, and mobile payment have become the main methods for people's daily transactions. For example: international online auctions and online shopping platform eBay 2019 first quarter results show that eBay active buyers increased by 4%, the total number of active buyers worldwide reached 180 million [1].

In the trend of e-commerce and remote transaction, the establishment of an open and transparent management platform for the transaction of corporate or personal assets is becoming more and more complicated. The main difficulties of centralized asset trading platforms are as follows: first, for both buyers and sellers, there is a big default premise that the third-party trading platform is safe and credible, and they are sure that it will operate impartially in the process of asset trading between the two parties. Secondly, the information of buyers and sellers is asymmetric, and the information of buyers is seriously lacking [2]. Furthermore, traditional asset transactions rely on entity credentials. And the anti-counterfeiting authentication process is complicated and has a long period of time. Besides, there are also problems of time-consuming and labor-intensiven in the process of circulation of user assets, requiring third-party organizations to participate at the same time and throughout the process. Finally, the sensitive data of both parties is widely controlled by third-party service organizations, and user privacy data has serious risk of disclosure [3].

Blockchain is a distributed data storage technology that includes P2P, asymmetric encryption, and consensus mechanisms. Its greatest features are decentralized and immutability [4]. In the era of blockchain 2.0, the integration of smart contract technology enables blockchain technology to have programmable features for different application scenarios, and to realize the advantages of pre-arranged and automated execution of both protocol rules [5]. The use of blockchain data distributed storage and immutable features can attract more users to upload their own personal data, to complete the function of information aggregation, to mine price and to share data onto the asset trading platform. Furthermore, the smart contract, which let blockchain can be programmed, enables two parties to reach an agreement in advance. Thus it meets system specifications and third-party service needs. Therefore, the blockchain technology is can be applied to solve the bottleneck problem of the current asset trading system, which can stimulate to meet the free exchange of corporate or personal assets and achieve the maximum utilization of social resources.

In order to reduce or even eliminate third-party, trusted or not, we introduce a blockchain-based asset trading system that can protect the asset security and identity security of both parties. Our contributions are three-fold:

- We first present the asset trading system without third-party 's services, which included designing and implementing smart contracts for asset release and asset trading.
- Based on the game theory, we further propose asset transaction matching model to find equilibrium solution that is optimally profitable for both buyers and sellers of asset transactions by calculating the user's reputation value.
- At last, we test and evaluate the throughput, the latency and the success rate of request response of smart contracts for asset release and asset trading.

978-1-7281-2542-8/19/$31.00 ©2019 IEEE
DOI 10.1109/CyberC.2019.00045

The feasibility of the system into actual production is demonstrated.

The rest of the paper is organized as follows: Section II briefly introduces background and related works; Section III describes the overall architecture of asset trading system and the operational flow of assert trading; Section IV presents the design of the asset trading system based on blockchain in detail, and introduces the development of smart contracts in the asset release phase and asset trading phase, and proposes a game-based matching model for buyers and sellers. Section V evaluates and tests the built system from two aspects of security and performance, and gives a performance analysis report. Section VI makes a summary and puts forward some future work.

II. Background and Related Work

A. Background on Blockchain

Blockchain was mentioned in 2008 by a self-proclaimed S. Nakamoto [6] was first used as a "ledger technology" at the bottom of Bitcoin to ensure that Bitcoin can still work normally after several hacking attacks. V. Buterin [7] proposed the next generation of Ethereum blockchain platform with code writing and automated operation smart contract technology. Ethereum multiple distributed nodes can implement smart contracts. Hyperledger Fabric [8] is led by IBM and Intel technology giants to build a single or multiple alliance chains to meet the business needs of the enterprise. The internal nodes need to be authenticated by the Fabric CA Client and the system is more private. EOS [9] is a blockchain architecture developed by block.one team. They invented blockchain architecture, similar to operating system, that can be used to authenticates, database read and write, asynchronous communication, and scheduling requirements for applications spanning multiple CPU cores or clusters. Known for the high throughput rate of millions of transactions per second and the fact that users do not pay fees.

These typical blockchain platforms have been developed to reduce the barriers to the use of blockchain technology, attracting more engineers and scholars to study [10].

B. Related Work

As for asset trading, previous work pursued efficient processing. P.C. Sun et al. [11] proposed a new Core Broking Model (CBM) to solve the group trading problem in e-markets. It mainly designed a combination model of multiple service providers to achieve a win-win-win situation for customers, providers and brokers. However, the authenticity of the transaction can not be guaranteed. S. R. Kim [12] mainly utilized blockchain's smart contract technology to ensure efficient and transparent transactions between government, real estate developers and users. Combining relevant laws with regulations of the Korean real estate market, they furthermore proposed a set of smart contracts and a related protection system to protect the interests of real estate traders. L. Xu et al. [13] mainly focused on the method of encryption to hide the traces of asset token exchange, and features of blockchain to ensure the fairness of asset transactions. By analyzing the relationships between stakeholders in the Kenyan retail trade sector, A. Kinai. et al. [14] built a blockchain platform that combine blockchain with mobile computing technology, to provide financial products and financial products services to SMEs. K. Mannaro et al. [15] presented the application of blockchain technology in the energy trading market, especially in smart grid trading. They utilized crypto-currency technology and smart contract technology to solve problems that the inconsistency between regional energy distribution and distributed production as well as the mutual transaction. A. Kosba et al. [16] designed a distributed smart contract system, Hawk. In order to ensure the security of transaction privacy, original financial transaction information is not stored in the blockchain, and the encryption protocol can be constructed by Hawk programmers. E. B. Sasson [17] applied a commitment function to encapsulate the source, destination and amount of each transaction into several parameters, and made use of the zero-knowledge proof technique zk-SNARKs to prove the transaction. It is not necessary to know the specific content of the transaction and related information when proving the transaction, so that the sender, payee and transaction amount of the blockchain transaction can be hidden.

In summary, the research and development of blockchain development platform is relatively mature, but the application research of asset trading is still in the early stage.

Considering transaction privacy, we choose Hyperledger Fabric as the underlying development platform for blockchain. In order to product the fairness of both parties to the assert, we develop smart contract for assert release and assert trading. Furthermore, to maximize the interests of both buyers and sellers, we propose asset-transaction matching model based on the game theory.

III. Asset Trading System Model

In this section, we introduce the architecture of the system for the first time, especially data storage. Then we show the operational flow of assert trading.

A. Architecture of Asset Trading System Based on Blockchain

The architecture of a blockchain-based asset trading system is shown in Fig. 1. The main players in the system are buyers and sellers of asset transactions. Buyers and sellers constitute an alliance chain of asset transactions, which aims to share asset information and achieve liberalized trading.

- **Buyer:** The buyer decides whether to participate in the bidding of a particular asset by browsing multiple seller asset information. The buyer's matchable range is determined by the buyer's reputation value. And then, the buyer and seller are matched by auction to complete the asset transaction. Finally, new asset certification information is generated. A digital digest of transaction information and new asset certification information are stored in blockchain to prevent modifying the information.

This mode provides evidence for possible legal disputes.

- **Seller:** The seller release the assets under his name by filling out and uploading the asset certification information. Then a digital digest of the asset information and its certification information are stored in the blockchain. This process enables users to share asset information and selling asset.
- **Data storage:** Asset release information and transaction information are stored in blockchain. Nodes that belong to the alliance chain can share asset release information and transaction information. Simultaneously, it can also provide evidence for possible legal disputes. Asset proof materials are stored in a separate database to prevent data modification and have easy management.

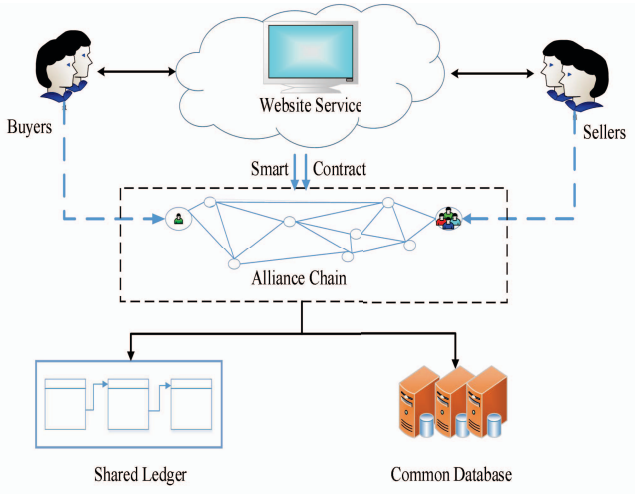


Figure 1. Overall Architecture of Asset Trading System.

B. Model Design of Asset Trading System Based on Blockchain

The asset trading system based on blockchain mainly consists of four phases, namely: system startup phase, asset release phase, buyer-seller matching phase, and asset trading phase. The operational flow of system is shown in Fig. 2, which is simplified flowchart and reflects the relationship between the concrete phase of assert trading system and involved transactions.

IV. Design Details of Asset Trading System

In order to achieve easy understanding and keep the exposition simple, we present the detailed process of each stage of the asset trading system.

A. System Setup Phase

When the asset trading system starts, the buyer and seller nodes join the blockchain network for the first time, and then initialize parameters, such as the organization of the node, the configuration block file, the creation of the application channel, and the installation of the smart contract.

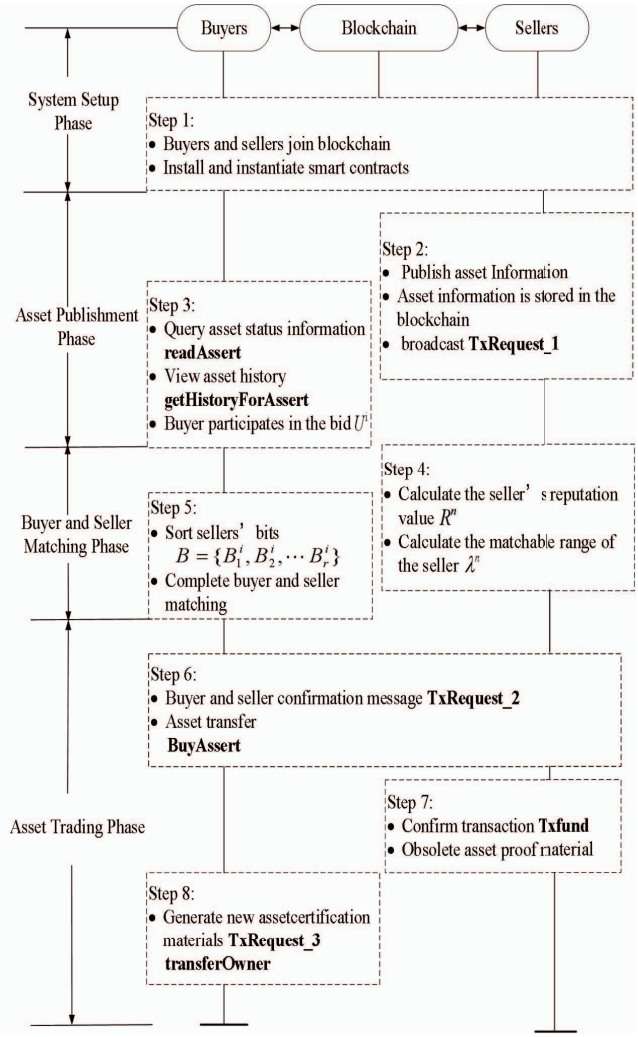


Figure 2. Operational Flow of Assert Trading

B. Asset Release Phase

The asset release phase refers to the entire process of the seller successfully publishing asset information and storing the asset hash value in the blockchain, which aims to share asset trading information. It mainly includes asset information inquiry, filling in asset information, and asset information storage in the blockchain. Its asset release process is shown in Algorithm 1.

The seller fills in the asset transaction information at first, then uploads the asset certification materials, finally stores them in a separate database. The hash value of the asset proof material is obtained by the MD5 hash algorithm, and the hash value of the asset summary information and the asset proof information is packaged into the blockchain ledger. Storing original information of assert and information hash values to prevent modifying information and improve query speed. The block information is signed and confirmed using the ECDSA digital signature. Thereby it completes the storage process of the asset release information onto the blockchain.

The seller can share assert information on blockchain, such as query asset history information. It takes measures of key-values for iterative query, where assert name is used as the key.

Algorithm 1 Assert Release

Input: asset type, asset name, sales amount, asset status, asset owner, asset certification information
Output: a prompt message of whether to deposit in the blockchain

```
1  if Whether the asset released by the asset name index;
2     return Asset already exists;
3  else Calculate the MD5 of the asset certification information;
4       Asset information is serialized;
5       Converted to json format;
6       Asset information is stored in the blockchain in the form
                of "asset name-asset sequence" key-value;
7       return asset successfully written to blockchain ledger.
8  end if
```

C. Buyer-seller Matching Phase

The buyer-seller matching model based on game theory mainly achieves the matching between buyers and sellers by calculating user's reputation value. Thus, the buyer/seller ratio of $n:1$ is transformed into $1:1$ in this process. It provides technical support for subsequent asset transactions that can invoke asset trading smart contracts.

The seller participates in n transactions, the n bid is recorded as U^n, the history of the seller's selling price, which can be recorded as a vector $U=[U^1,U^2,\cdots,U^n]$ and satisfied with

$$U^1 \geq U^2 \geq \cdots \geq U^n \tag{1}$$

In other words, the seller wants the higher the price of the product. However, if the transaction is not complete in the previous round, the round of bidding needs to be lowered to complete the transaction.

Suppose r buyers makes n round of bidding to complete bidding, then the n round of r buyer recorded as $B=[B_1^n,B_2^n,\cdots,B_r^n]$, the history of the k buyer's bid, recorded as $B_k=[B_k^1,B_k^2,\cdots,B_k^n]$, and satisfied with

$$B_k^1 \leq B_k^2 \leq \cdots \leq B_k^n \tag{2}$$

This means that the less money the buyer wants to buy asset. If the transaction is not completed in the previous round, the buyer needs to be raised to bid to complete the transaction.

r buyers winning result can be recorded as $X=[x_1,x_2,\cdots,x_r]$, x_i is a binary number, $x_i=1$ means winning the bid, and $x_i=0$ means not winning the bid.

The n round bid winners must satisfied with

$$B_k^n \geq U^n \tag{3}$$

Obviously, the buyer's bid must be greater than or equal to the seller's price, and the bid may be win.

The transaction price of the n bid is marked as p, then the profit of the seller is recorded as

$$W=(B-P)\cdot X \tag{4}$$

The buyer's profit is recorded as $P-U$.

The history of the participant's reputation value can be recorded as $R_k=[R_k^1,R_k^2,\cdots,R_k^n]$, and the reputation value of the n round of bidding participants is calculated as

$$R_k^n=\frac{1}{2}\cdot\left(\frac{\delta_k^n}{\theta_k^n}+\frac{\theta_k^n}{t_k^n}\right) \tag{5}$$

Where δ_k^n represents the number of favorable votes received by the participants before the n round of bidding, θ_k^n represents the total number of actual transactions before the n round of bidding, and t_k^n represents the participant's bidding transaction number before the n round of bidding. $R_k^n \in (0,1]$, R_k^n is closer to 1, indicating that the participant's reputation value is higher.

The matchable range of the buyer's n round of bidding is recorded as

$$\lambda_k^n = N^n \cdot R_k^n \tag{6}$$

Where N^n represents the number of people actually participating in the bidding for the n round.

The matching process between buyers and sellers is shown in Algorithm 2.

In Algorithm 2, from Line 1 to Line 5, mainly calculate buyer's matchable range λ^n by using (5) and (6). It means that deciding buyers and sellers to complete the match, mainly considering the user's reputation value and bid amount. If this round does not complete the match, buyer and seller will restart bid or seller will stop bidding.

Proof: When the interests of buyers and sellers are optimal, the transaction price P must be satisfy with $\lim_{n\to\infty} P=(B_{\max}+U^i)/2$.

It is known from the above that the buyer wins the bidder $B_{\max}$ (refers to the buyer with the largest bid amount in the bid collection after removing the discrete value), the buyer profit is $B_{\max}-P$, the seller profit is $P-U^i$, the total profit of the k round bid market is $B_{\max}-U^i$, so within the matching range, when the interests of buyers and sellers are optimal, the transaction price should be satisfy

with $\lim_{n\to\infty} P = (B_{\max} + U^i)/2$.

Algorithm 2 Matching buyers and sellers

Input: price U^i, bid collection $B = \{B_1^i, B_2^i, \cdots B_r^i\}$, participant k reputation value R_k^n

Output: Transaction price P, winning result X, seller profit W, buyer profit $P - U$

```
Remove values less than U^i in B;
Sort B in ascending order;
λ_k^n = N · R_k^n;
num = round(λ_k^n);
Remove discrete points in the collection B;
if num == 1
    p = max(B);
else
    temp = inf
    for each η ∈ {b_1, b_2, ⋯ b_num}
        cur = η − (B_max + U^i)/2;
        if cur < temp
            temp = cur;
            p = η;
        end if
    end for
end if
```

D. Asset Trading Phase

The asset trading phase is mainly divided into the buyer's request for the transaction, the seller's response to the transaction and the proof of the old asset, and the production of new asset certification materials. Among them, requesting transactions, responding to transactions, and generating transactions are all carried out on-chain, and the proof of the old assets and the production of new certification materials are carried out off-chain. The asset trading phaseis shown in Algorithm 3.

Algorithm 3 Asset trading

Input: seller name, buyer name, transaction price
Output: a prompt message of whether the transaction is successful or not

```
Deserialize buyer information;
Sort B in ascending order;
if P > buyerJSON. Account
    return fail;
else
    Deserialize buyer information;
    buyerJSON.Account = buyerJSON .Account - price;
    sellerJSON.Account = sellerJSON.Account + price;
    buyerJSON.Success_number++ ;
    sellerJSON.Success_number++;
    Serialize buyer and seller information;
    Buyer, seller serialization information is written to the blockchain;
    return success.
end
```

V. Performance Evaluation

An asset trading system based on the Hyperledger Fabric platform is built on the Ubuntu 16.04 environment servers with 2G memory and 2.20 GHz processor. In order to test and evaluate the security, function and performance of the blockchain-based asset trading system, Postman and Hyperledger Caliper were used for system function testing and performance testing respectively.

In this paper, the network topology structure of the blockchain asset trading system is as follows: there are two organizations that represent the asset trading buyer and seller. Each organization has two peer nodes, an orderer sorting service node, a certificate authority (CA). Asset trading participants join the blockchain network as peer node, installing smart contracts, and instantiation. The orderer node is mainly responsible for the function of sorting, packing, and reaching consensus of the block. The CA authentication node is mainly responsible for issuing the public key and the private key, and determining whether the user can join the blockchain network.

The asset release, the matching of asset buyers and sellers, and the asset trading function are realized. The integrity and traceability of asset transaction records are ensured by the features of the blockchain such as immutability and traceability. Due to environmental constraints, the throughput of the test system is approximately 90 TPS (TPS represents the transaction volume per second in the actual production environment).

A. Security Analysis

The blockchain asset trading system built in this paper is based on the Hyperledger Fabric development platform. The writing and query of asset information are all operated by invoking smart contracts, and the corresponding blocks will be generated. The block information includes the operator's digital signature information, and the two blocks are connected in series by hash values. Therefore, all operations of the asset trading participant are recorded in the block and can not be modify.

If a semi-honest participant exists in an asset trading and attempts to infer information outside the agreement through the information of the agreement, the operational record of the semi-honest participant is stored when the asset information is queried or other smart contracts are invoked. Otherwise, he is unable to obtain any asset information. It provides evidence for potential accountability for privacy breaches or other malicious consequences.

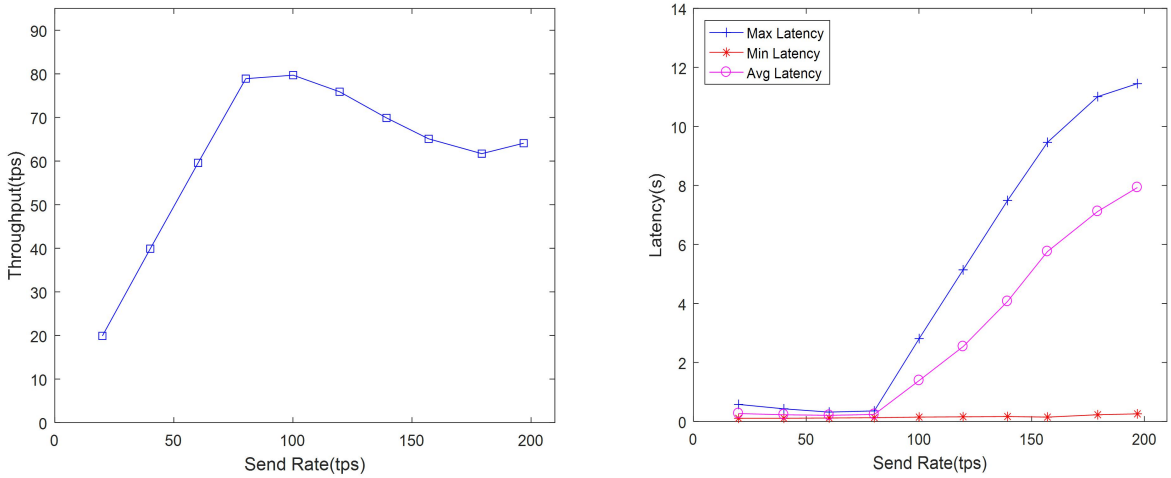
B. System Performance Testing and Analysis

Based on blockchain, the operation of the system is completed by invoking smart contract of the system to complete the access of the block data. In this regard, the performance of the asset initialization function based on the block data writing and the asset query function of the block data reading are tested separately. Among them, the main performance indicators include the latency of invoking the chaincode, the throughput and the success rate of the event request response.

Fig. 3 shows the performance test results of the asset release storage function. Among them, Fig. 3(a) shows the relationship between the send rate and the throughput of the asset release storage function. It can be find that the maximum throughput of the system is close to 90tps. Then, as the send rate increases, the system throughput is gradually reduced. Fig. 3(b) shows the relationship between the send rate of the asset release storage function and the latency. It can be seen from the figure that when blockchain asset trading system initially stores information, there is network jitter. Before the system fails to reach the processing bottleneck, the system latency tends to be gentle, and the average latency is less than 0.27s. As the send rate increases, the average latency increases significantly. The main reason is that the request transaction queues up and the latency is increased.

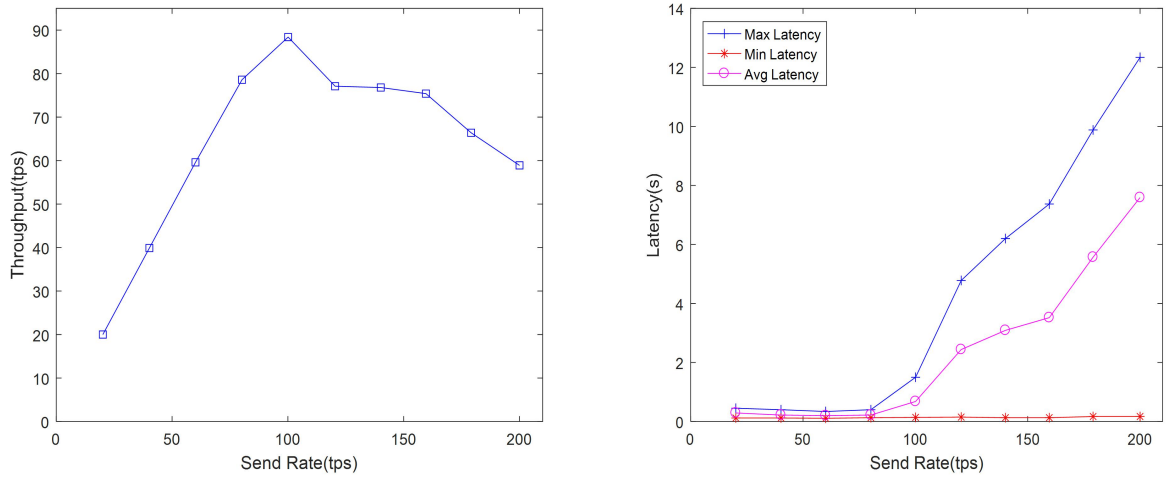
Fig. 4 shows the performance test results of the asset trading query function. Among them, Fig. 4(a) shows the relationship between the send rate and the throughput of the asset trading query function. It is obvious that the throughput of the blockchain read function is slightly higher than the write function's throughput, when the system throughput bottleneck is not exceeded. Fig. 4(b) shows the relationship between the send rate and the throughput of the asset transaction query function, which is the same solution as the asset release storage function.

Fig. 5 is the relationship between the send rate and the success rate of the request event response. When the maximum throughput of the system is not exceeded, the success rate of the event response is 1 basically, and the system performance is good. When the system is overloaded, the success rate of the event response is gradually reduced. It is mainly caused by the timeout of the event request.



(a) Transaction send rate and throughput (b) Transaction send rate and Latency

Figure 3. Asset Publishment Storage Function Performance Test Results



(a) Transaction send rate and throughput (b) Transaction send rate and throughput

Figure 4. Asset Trading Query Function Performance Test Results

In summary, by analyzing the performance of the storage function and query function of the blockchain asset trading system, the throughput of the system is close to 90TPS due to the limitation of the test environment. And when the system does not exceed the send rate processing bottleneck, the system's average latency is less than 0.27 seconds, and the success rate of the event response is 1 basically.

However, if reduce the network topology and select better servers ,the maximum throughput of the system will be improved to a certain extent. And the system performance is good when the maximum throughput of the system is not exceeded.

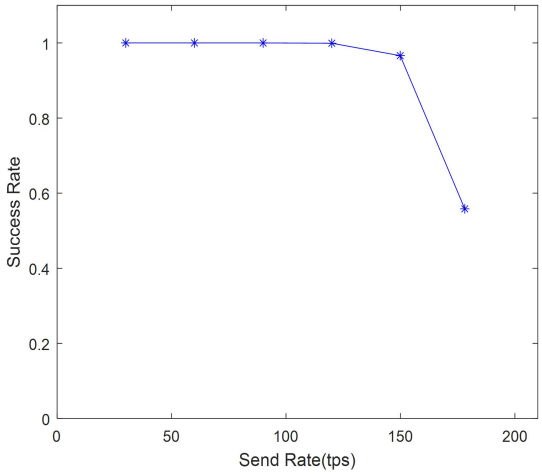


Figure 5. Relationship Between Send rate and Event Response Success Rate

VI. CONCLUSION

Our main job is building an asset trading system based on the Hyperledger Fabric platform. To be specific, an asset trading system architecture and the overall process based on blockchain technology were proposed at first. Secondly, by studying game theory and user reputation value, we designed the matching model of asset trading and found the equilibrium solution of profit-seeking between buyers and sellers. Then we implemented smart contracts for asset release and asset trading. Finally, we tested and evaluated the function and performance of the system, which demonstrated the feasibility of the system being put into actual production .

In the future, our work is mainly to improve the functions of the system, to protect user privacy and improve user friendliness.

ACKNOWLEDGMENT

This work is supported by National Natural Science Foundation (Grant No. 61772099); the Program for Innovation Team Building at Institutions of Higher Education in Chongqing (Grant No.CXTDG201602010); the Chongqing Science and Technology Innovation Leadership Support Program (Grant No. CSTCCXLJRC201917); the University Outstanding Achievements Transformation Funding Project of Chongqing (Grant No. KJZH17116); the Artificial Intelligence Technology Innovation Important Subject Projects of Chongqing (cstc2017rgzn-zdyf0140); the Innovation and Entrepreneurship Demonstration Team Cultivation Plan of Chongqing (cstc2017kjrc-cxcytd0063); the China Postdoctoral Fund (Grant No.2014M562282); the Project Postdoctoral Supported in Chongqing (Grant No. Xm2014039);the Science and Technology Research Project of Chongqing Municipal Education Committee (Grant No. KJ1704089); the Chongqing Research Program of Basic Research and Frontier Technology (Grant No. cstc2017jcyjAX0270, Grant No. cstc2018jcyjA0672, Grant No. cstc2017jcyjAX0071); the Industry Important Subject Projects of Chongqing (Grant No. CSTC2018JSZX-CYZTZX0178, Grant No. CSTC2018JSZX-CYZTZX0185).

REFERENCES

[1] eBay Inc. "Reports first quarter 2019 results"s. 2019, [EB/OL], https: //www.ebayinc.com/ stories/ news/ebay-q1-2019-results/.

[2] J. H. Han and H. M. Kim, "The role of information technology use for increasing consumer informedness in cross-border electronic commerce: an empirical study," Electronic Commerce Research and Applications, Vol.34, pp. 1-16, 2019.

[3] T. Glenn and S.Monteith, "Privacy in the Digital World: Medical and Health Data Outside of HIPAA Protections," Current Psychiatry Reports, Vol. 16, pp. 494-505, 2014

[4] Z. B. Zheng, S.A. Xie , Dai , and Wang H. "Blockchain challenges and opportunities: a survey," International Journal of Web and Grid Services. Vol. 14, No. 4, 2018.

[5] C. Konstantinos and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," IEEE Access, Vol.4, pp.2292-2303, 2016

[6] S. Nakamoto, "Bitcoin: "A peer-to-peer electronic cash system," 2008. [EB/OL]. http:// bitcoin. org/bitcoin.pdf.

[7] V. Buterin, "A next-generation smart contract and decentralized application platform,"white paper, 2014. [EB/OL]. https:// github.com/ ethereum/wiki/wiki/White-Paper.Article in a conference proceedings

[8] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin , C. Konstantinos, et al. "Hyperledger fabric: a distributed operating system for permissioned bockchains," 13th EuroSys Conference (EuroSys 13). Apr.2018, doi:10.1145/3190508.3190538.

[9] EOSIO. ″ EOS.IO Technical White Paper, ″ 2018 , [EB/OL], https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md.

[10] J. Yli-Huumo, D. Ko, S. J. Choi,S.Y. Park, and K. Smolander. " Where is current research on blockchain technology?—a systematic review,".Plos one. Vol.11, pp.1-27. 2016. dot:10.1371/ journal. pone.0163477

[11] P. C. Sun, M. Odetayo, R. lqbal, et al. "a core broking model for e-markets," International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. Oct. 2012, pp.249-256, doi:10.1109/CyberC.2012.49

[12] S. R. Kim, "Smart contract system by Blockchain of real estate transaction". Korea Association of Real Estate Law. Val.22, No.3 ,pp. 93-124, 2018

[13] L. Xu, L. Chen, N. Shah, et al. "Zero Trade: Privacy Respecting Assets Trading System based on Public Ledger," .21st International Workshops on Financial Cryptography and Data Security.2017.

[14] A. Kinai, M. Isaac, O. Erick , et al. "Asset based lending via a secure distributed platform,". the Ninth International Conference on Information and Communication Technologies and Development. 2017 ,pp16-19, doi:10.1145/3136560.3136594

[15] K.Mannaro, A.Pinna, M.Marchesi, "Crypto-Trading: blockchain-oriented energy market," AEIT International Annual Conference (AEIT), Sep. 2017, pp.20-22, doi:10.23919/AEIT.2017.8240547.

[16] A. Kosba , A. Miller , E. Shi ,Z. Wen, C. Papamanthou . "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts", IEEE Symposium on Security and Privacy(SP) , May.2016, pp.839-858, doi:10.1109/SP.2016.55

[17] E. B. Sasson, A. Chiesa ,C. Garman , et al. "Zerocash: Decentralized anonymous payments from bitcoin," 2014 IEEE Symp on Secuurity and Privacy . Piscataway, NJ:IEEE, May.2014,pp.459-474, doi:10.1109/SP.2014.36