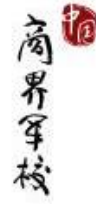




PHBS
北京大学汇丰商学院



Design of an online trading platform mechanism based on blockchain technology in China

Author: Yiming Jiang

Number: 2401212398

Dept: Fintech, PHBS

Course: Introduction to Fintech

Date: 2024.11.3

1. Abstract

This article designs a blockchain-based online trading platform in China, leveraging the characteristics of data transparency and distributed ledger technology, while considering Chinese domestic policy regulations and consumer habits. Under this mechanism, incentivized by economic rewards such as coupons and discounts, transaction records will be jointly recorded and maintained by platform users, thus reducing the platform's bookkeeping and storage costs. Additionally, since transaction data is visible to all users, the often-contentious issue of price discrimination is expected to be resolved. Finally, a membership system is introduced to enhance platform profitability and user experience, while also allowing the platform to intervene in order to address conflicts between virtual transactions and the delivery of actual goods.

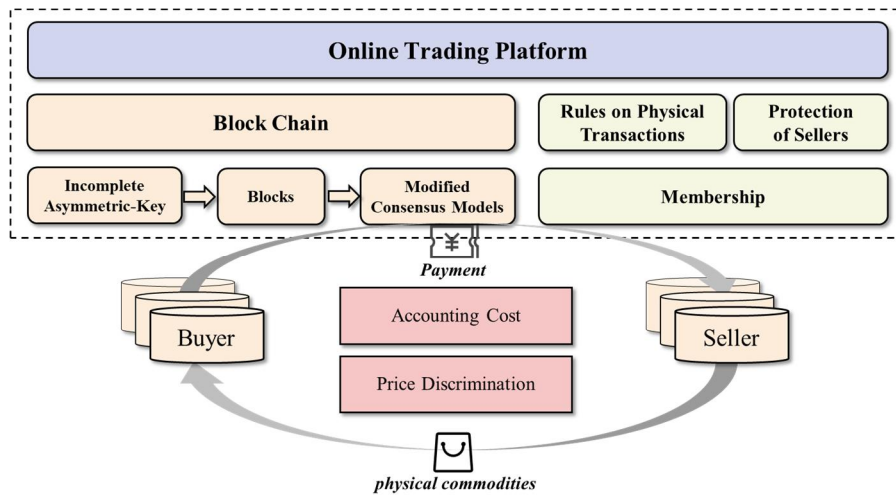


Fig 1. Architecture of Online Trading Platform.

2. Background and Introduction

China has many well-known online trading platforms, such as JD.com, Taobao, and Pinduoduo. In the traditional operational model of these platforms, each platform establishes and maintains its own database to store transaction information, product details, and other data, which incurs significant costs. During daily operations, these platforms generate profit by running advertisements, charging transaction fees, service fees, and membership fees^[1]. However, for consumers, there is the risk of price discrimination if platforms or sellers accumulate sufficient data to determine consumers' economic standing and payment capacity,

potentially increasing platform revenue at the consumer's expense^[2].

To address these two major issues, I propose the concept of a blockchain-based online trading platform mechanism. This approach allows the platform to significantly reduce the costs of database maintenance, and product pricing will be transparent, as all users will be able to see all transaction data. This paper will elaborate on the details of this mechanism and analyze the associated risks and potential benefits.

3. Storage Medium: Block Chain or Database

Since product information is frequently updated by sellers due to new product releases, the sale of older products, price adjustments, and modifications to product descriptions, this conflicts with the tamper-resistant nature of blockchain, so the blockchain should not be adopted, a database will still be used to store product information. On the other hand, because transactions once completed should not be altered, it is feasible to use blockchain for recording transaction information. Additionally, considering that unregistered users should not be allowed to conduct transactions on the platform, the blockchain will be designed as permissioned. Registered users who conduct transactions with sellers will have the right to publish transaction information to the blockchain network, while sellers will retain the ability to operate the database to update their product information.

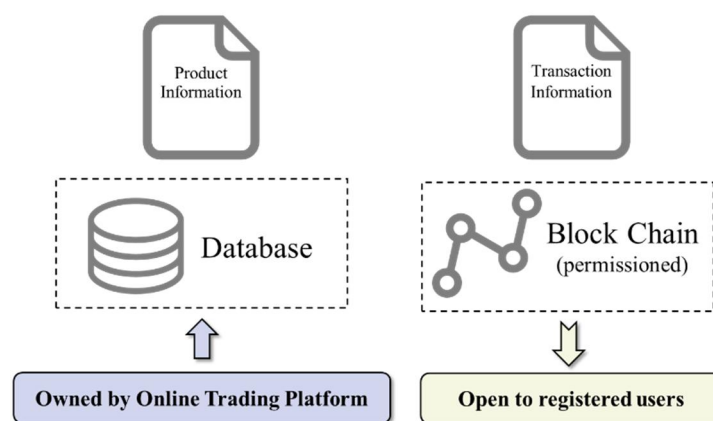


Fig 2. Data storage and usage permissions.

4. Incomplete Asymmetric-Key Cryptography

According to Chinese policies or laws, complete anonymity may not be allowed. Therefore, users first need to visit relevant government departments for verification to obtain a private key,

which will then only be known by the government and the user. In the event of any illegal activity, the government can hold the user legally accountable. After obtaining the private key, users can store it in software or a digital wallet. Generally, once a private key is lost, it cannot be retrieved. However, in this case, since the government also holds the user's private key, users can use their identification to retrieve it if necessary, preventing financial loss due to forgotten private keys. Additionally, the user with high membership levels can receive an extra symmetric encryption key from the platform, which is also shared with the sellers they wish to trade with, they can use this key to encrypt their transaction information and broadcast it to the blockchain network. As premium membership is highly appealing, the platform can generate substantial revenue through the membership system.

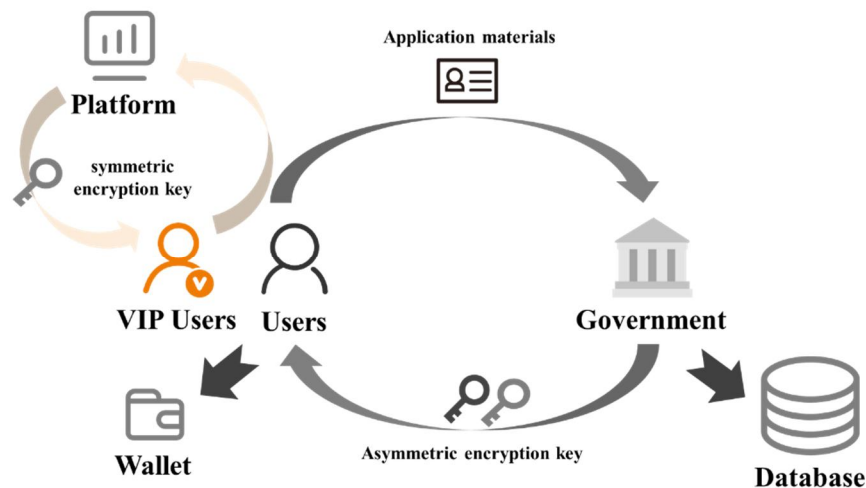


Fig 3. The government and users will simultaneously hold the same private key. Users in high membership can get extra symmetric encryption key from the platform.

5. Blocks

Since cryptocurrency is not permitted in China, transactions on this platform are still based on the RMB. Buyers need to transfer sufficient funds to their wallets on the platform before making purchases. When a transaction occurs, the buyer uses their private key provided by the platform to encrypt the transaction information, generating a transaction record that includes transaction details. This information may include the order number, sender address, recipient address, product details, unit price, total amount, transaction time, maximum waiting time, transaction channel (to be discussed further below), and tracking number (as proof of shipment

by the seller). The signed transaction is then broadcast to the blockchain network, where it awaits node verification, block creation, and addition to the blockchain.

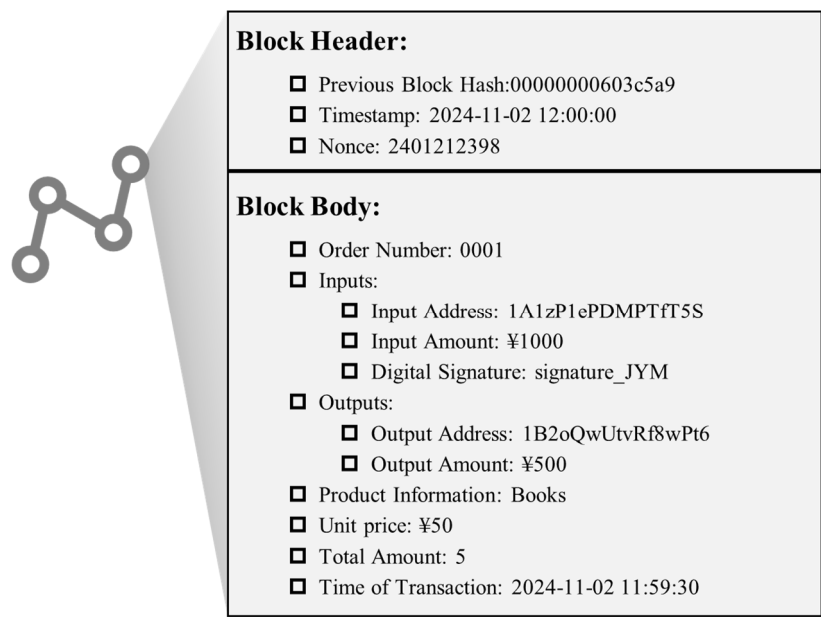


Fig 4. An example of the block in blockchain.

6. Modified Consensus Models

When determining which user will publish the next block, considering the principles of well-known models like the Proof of Work Consensus Model^[3] and the practical situation in China, I would like to introduce the Government-Supervising Proof of Credit-Membership Consensus Model. In this model, users with high credit and high membership levels are regarded as more reliable and are thus more likely to be selected to create blocks. Scores are calculated through a weighted combination of credit and membership level; the higher the score, the greater the probability to be selected.

In each round, multiple users are chosen to create blocks, and then all users participate in voting to determine which block to adopt. Contributors to the chosen block receive coupons or discounts from the sellers listed in that block, and their credit score also increases. Conversely, those who engage in malicious actions will face penalties such as credit deductions or even expulsion from the blockchain network. The entire process is under government supervision; if the government deems any action risky or illegal, the created block will be rendered invalid.

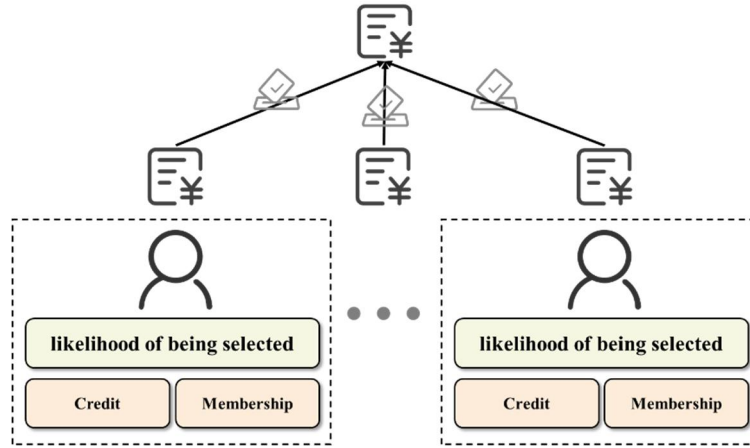


Fig 5. Government-Supervising Proof of Credit-Membership Consensus Model.

7. Physical Transactions and Returns

In order to ensure that the commodities that consumer bought will be shipped normally, rather than the seller not sending anything after receiving payment, the platform supports two types of transactions. If the buyer does not trust the seller, they can choose the platform as an intermediary for the transaction. In the buyer's transaction information, the recipient should be clearly listed as the platform, with a note specifying the final seller account and the maximum wait time. The platform, backed by its own assets and reputation, collects the payment for the product from the buyer along with an additional percentage as a transaction fee. The platform then broadcasts the product purchase information, and once the seller receives it, they should prepare and promptly ship the item, broadcasting the shipping information, including the tracking number. This information is recorded by user nodes into a block and added to the blockchain. If the shipping time does not exceed the wait period specified by the buyer, the transaction is confirmed; otherwise, the platform will broadcast a transaction cancellation notice. In case of a failed transaction, the platform will refund the payment to the buyer, though the transaction fee may be partially retained.

Even if the transaction is successful, the payment from the platform to the seller will not occur immediately; it will wait until the buyer confirms receipt or until a specified period elapses without a refund request. Sellers with higher membership levels may request a shorter waiting period. Upon completion, the platform will deduct a portion of the transaction fee from the seller's declared sale price before transferring the remaining amount to the seller. If the

buyer requests a refund after receiving the item but before the end of the specified period, they must broadcast the return shipment tracking number. The platform will then refund the payment to the buyer, with the transaction fee partially retained as appropriate.

On the other hand, if the buyer and seller have a long-term cooperative relationship or the seller has a good reputation, the buyer may opt to bypass the platform and transfer the payment directly to the seller's address, awaiting shipment afterward. In case of a return, the buyer and seller must negotiate directly.

In the process described above, higher-level member buyers will enjoy lower transaction fee, with the possibility of a full refund of the transaction fee in the event of a failed transaction. Additionally, higher-level members can set shorter waiting times for receiving goods and may even specify the logistics company for shipping within a reasonable range.

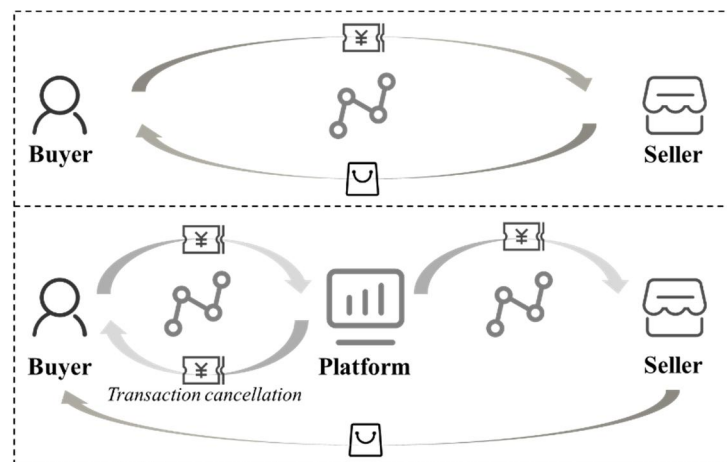


Fig 6. Two ways of transaction.

8. Price Discrimination

Due to the distributed ledger nature of blockchain, the platform has addressed data storage issues to a certain extent. Regarding price discrimination, the transparency of transaction data allows all users to access historical transaction information through the platform software to view prices of similar products. Excluding the impact of inflation and product costs, if unreasonable pricing by a seller is discovered, users can report it to the platform. Once the platform accepts the report, it may reduce the seller's reputation score accordingly. A lower reputation score means that buyers are more likely to choose to transact through the platform, which incurs higher transaction fees. Additionally, the platform's monthly or annual service

fees for the seller will increase. If price discrimination is severe, the seller risks being expelled from the platform or being reported to the State Administration for Market Regulation.

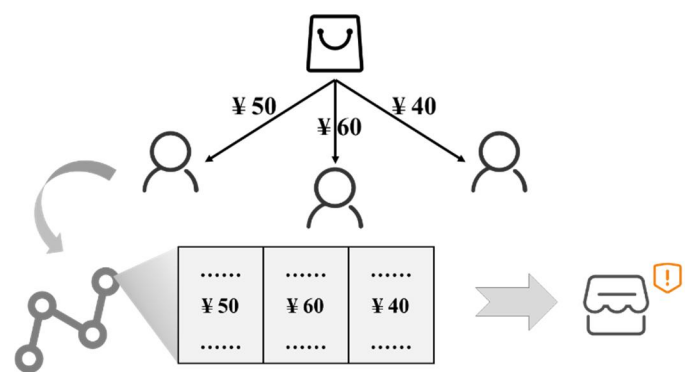


Fig 7. Price discrimination and countermeasures.

9. Protection of Sellers

The measures mentioned above, such as issuing coupons to record keepers and combating unreasonable pricing by merchants, seem to impose harsh requirements on sellers compared to existing platforms, which may be detrimental rather than beneficial. To attract merchants and ensure their sustained operation, this platform can allocate a portion of the cost savings from data storage to subsidize reputable but heavily loss-making or newly onboarded merchants, while also reducing service or advertising fees charged to sellers compared to other online trading platforms. Additionally, the platform can redirect more technology and resources away from data storage and bookkeeping to develop a more user-friendly interface for buyers and sellers, enhancing the overall user experience.



Fig 8. Measures to protect sellers.

10. Risks

Malicious behavior of many users. When there are many users, theoretically, the security of information can be ensured through mutual verification and supervision among users. However, it is important to note that in the early stages of the platform, when there are fewer users, or when some users collaborate to engage in malicious behavior, there may be a risk of a 51% attack. In this scenario, malicious users could leverage their computational power to

compete and replace the real transaction chain with a longer blockchain, thus altering historical transactions. Additionally, they might also conspire to disregard certain users' transaction information, completely preventing those users from conducting transactions.

Incomplete decentralization. Although there are trading avenues that do not rely on a platform, if dependence on the platform exists, there is a risk that a central node could be attacked, leading to an overall collapse of the system.

Malicious behavior of platforms under regulatory deficiencies. The platform holds significant authority, and if supervision is inadequate, it could privately alter data or refuse to process certain users' transactions. On one hand, the government should actively intervene to strengthen regulation; on the other hand, it could also attract more publishing nodes by increasing economic incentives.



Fig 9. Three main risks of the mechanism.

11. Conclusion

This mechanism focuses on the two main features of blockchain: data transparency and distributed ledger technology, designing an online trading platform based on blockchain. Since transaction data is visible to all platform users, the issue of price discrimination is expected to be effectively resolved. Additionally, due to the distributed ledger, the platform can save on costs associated with recording and storing transaction information. This mechanism has made several adjustments to the original blockchain model, considering the actual situation in China.

Firstly, given that China does not allow the use of cryptocurrencies for transactions and those coupons and discounts are particularly appealing to Chinese users, we have changed the rewards for accounting from general cryptocurrencies to coupons or discounts from the sellers who receive payments in the blocks. Secondly, considering the prevalence of membership recharge culture in the domestic market, we have introduced a membership system into the mechanism, where users will enjoy a range of privileges such as transaction information

encryption, priority in accounting, lower fees, and shorter transaction waiting times based on their membership level. Finally, since completely anonymous transactions are not permitted in China, the private keys of the online trading platform will be held and managed by both users and government departments, which provides the benefit of being able to recover keys even if lost by contacting the government.

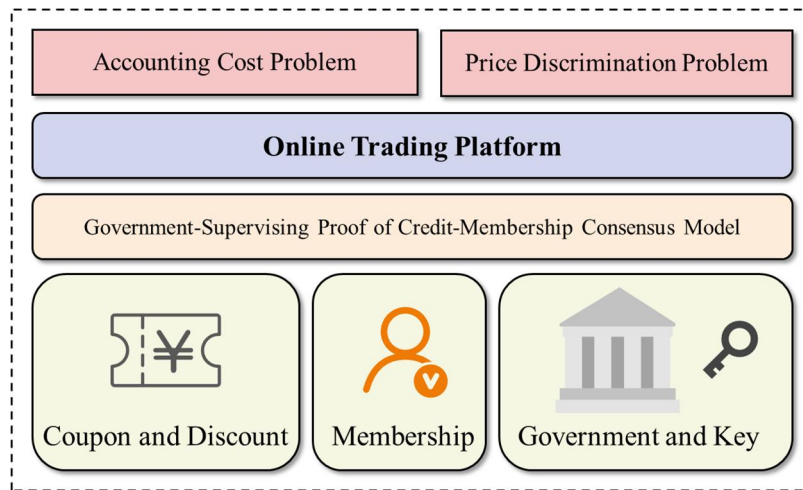


Fig 10. The main innovation points and problems solved by the mechanism.

However, we should also recognize that the blockchain itself is susceptible to risks like a 51% attack, which cannot be avoided in our mechanism. In summary, I believe this mechanism has certain application prospects and can play a role in reducing platform costs and protecting consumer rights. However, within the current industrial landscape in China, further discussion and research are needed on how to coordinate with government agencies, win users' trust, and survive competition with online trading platforms such as Tmall and JD.

12. Reference

- [1] Liu, Haoyuan, and Rui Xiao. "Research on the Development Problems and Countermeasures of China's E-commerce Platforms——Taking Taobao as an Example." BCP Business & Management, (2021)
- [2] Han, Wei, Yajie Gao, and Ai Deng. "Algorithmic price discrimination on online platforms and antitrust enforcement in China's digital economy." Antitrust Source, (2018).
- [3] Yaga, Dylan, et al. "Blockchain technology overview." arXiv preprint arXiv:1906.11078 (2019).