



渔翁系统白皮书

Fisher System Whitepaper

Version: v1.0
2022-03-20

1. Background

In 2008, the release of Satoshi Nakamoto's "Bitcoin: A Peer-to-Peer Electronic Cash System" (*Bitcoin: A Peer-to-Peer Electronic Cash System*) paper and subsequent software officially launched the Bitcoin financial system, followed by Bitcoin From the involvement of technology geeks to the hype army, the price of Bitcoin continues to break new highs, and the technology behind it has also been mined to become the continuous development of the blockchain concept.

In 2015, Ethereum brought the concept of smart contracts into the blockchain, and developed a variety of public chains that support scalability. A large number of economic models are proposed, and then various experimental systems are constructed. Instantly attracted the attention of capital, a large amount of capital rushed in, very lively. The proposal of the high-performance public chain system EOS has led to the largest public chain financing project in history.

Later, based on the application of DEFI on the public chain, the rise of cross-chain, NFT, etc. led to round after round of investment speculation.

Up to now, most of the DAPPs are speculating within the currency circle, and it is rare to see a system that solves problems in real life and improves efficiency in real life. The fisherman system proposed in this paper is indeed a use of blockchain smart contract technology to solve the trust problem in real life, which has great practical value. It can not only reduce the transaction cost between strangers, but also improve the security of the transaction.

2. System Introduction

The fisherman system is a system that generates virtual credit based on the smart contract of the blockchain public chain. It generates virtual credit by over-collateralizing valuable virtual assets and several logical combinations. Based on the generated virtual credit, users can realize safe exchanges or transactions. Anyone can generate their own credit through this system.

The naming of the system is inspired by an ancient Chinese fable: Sandpipers and clams compete for the fisherman's profit. It tells the story of two animals, mussels and snipe birds, fighting each other, and neither wanting to give in, but the fisherman who passed by finally got a bargain. Here, it is suggested that both parties to the transaction should stand on the other side's standpoint and understand the reasons and responsibilities of the dispute when encountering disputes. If they do not give in due to disputes, they eventually breach the contract. Then the sword of Damocles, the fisherman's contract, will fall, and both sides will suffer. In the end, the fisherman wins. Of course, the fisherman is a kind character, and the profits will be used for public welfare.

Name the system by borrowing from this profound and instructive fable. The system mainly solves two problems: First, users can mortgage assets safely through the "preset conditions" algorithm, without worrying about the malicious deception of the other party or others, and they will be locked and cannot be retrieved. Second, through the "and lock" algorithm mechanism, that is, the mechanism that both parties can unlock the asset can only be retrieved to realize that the defaulting party cannot be without loss, thereby ensuring the security of the transaction.

In real life, we all encounter the need for non-face-to-face transactions or exchanges between strangers. Especially now that the concept of the metaverse has spawned a lot of gameplay, and most players are communicating online, which will require exchanges or transactions. In a profitable environment, scammers are popular, and any credulousness may suffer losses. At this

time, a secure channel is needed as a third party to ensure safe transactions. In the past, when there was this demand, we often thought of professional third parties, such as ESCROW, Alipay, etc. But such third parties are expensive due to the cost of running a large team, and may charge much more than the exchange/trading price. It is also possible that they will not accept these small orders at all. In this case, the fisherman system can help you a lot, it is very low cost, but it is very safe, and it will not reject you because you are a small order. Because all of this can be controlled by both parties to the transaction.

Therefore, it can be imagined that this is a system with great practical value, which can be considered for all requirements related to credit security. It can solve the safe exchange of things and things, and it can also solve the safe transaction of things and money. The problem of exchanging virtual assets across chains can also be easily realized through this system. In the metaverse, it can be used as a bridge to connect the islands, between the metaverses, and between the metaverse and the real world. Another value of this system lies in its scalability. Various applications can be developed based on the concept of virtual credit to solve problems in specific fields.

Of course, to complete the above, you need patience to understand the unique design idea of the system, it is not complicated. The system can be implemented using a public chain based on smart contracts. Here we first implement it based on the EOS public chain to make full use of the unique performance advantages of EOS.

3. Function

The core function of the system is to generate virtual credit through over-collateralization and non-achievement, thus achieving the goal that the defaulter cannot have no loss. So to use this system to solve your problem, you need to have on-chain assets. The implementation process logic of the function is described below. In this model, the initiator is called the inviter, the inviter is called the invitee, and the fisherman protocol is the third party.

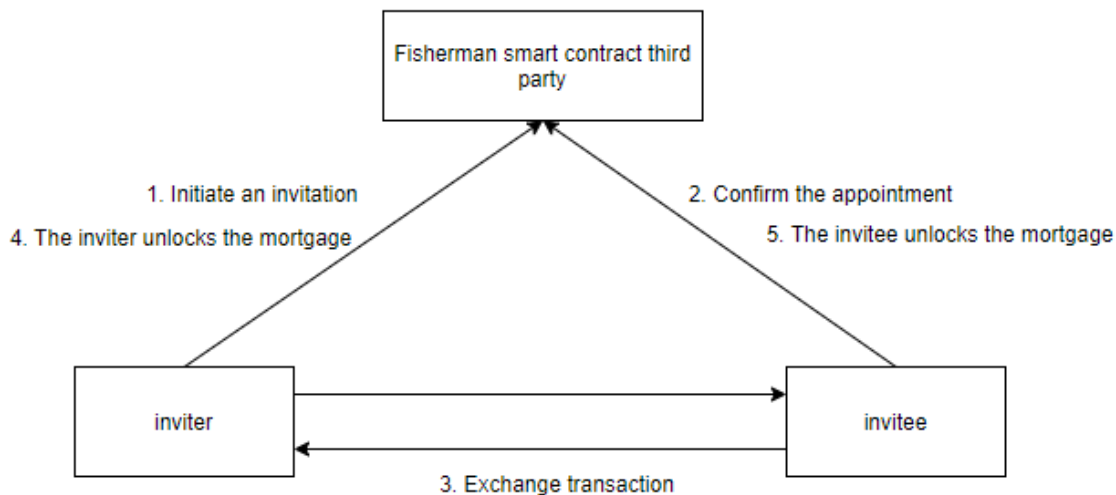


Figure 3. Business flow chart

1. After the consensus is reached, the transaction invitation party initiates a mortgage invitation to the smart contract. The invitation contains mortgage parameters, such as the number of mortgages and the invited account number.
2. After the respondent receives the invitation, check whether the mortgage parameters are consistent with the previous negotiation, and execute the contract action according to the mortgage parameters after confirmation.
3. The exchange of the transaction between the two parties can be initiated by any party first, as long as the negotiation method is finally realized and the exchange is successful.
4. After the transaction is successfully exchanged, the inviter unlocks the pledge of the respondent, and the unlocking action can also be performed by the inviter first, and the pledge cannot be retrieved at this time.
5. The inviting party unlocks the inviting party's collateral. After both unlocking the other party's collateral, both parties can retrieve the collateral, and the entire transaction process ends.

3.1. invitation

The design of the specified parameters in point 1 is to prevent others from maliciously calling the contract to lock your assets. If you do not specify the amount of collateral and the invited account number, others will call the contract to lock your assets without providing collateral assets, resulting in You can't get it back. The selection of the amount of collateral should make its overall value more than double that of the transaction, otherwise the security of the transaction cannot be guaranteed in the event of a default.

3.2. Invited

The second point is that the inviter needs to provide no less than the amount of collateral specified by the inviter to execute the lock successfully, otherwise the lock action cannot be performed. Once locked, the mortgaged assets can be retrieved unless both parties reach an agreement and both agree and execute the unlocking. If an agreement cannot be reached, or one party fails to perform as agreed, the other party should not unlock, otherwise it will suffer more losses. Take safety into your own hands with the Fisherman System. Of course, there will be various unforeseen problems in the actual exchange or transaction. At this time, both parties need to seek truth from facts, make some reasonable concessions or concessions in good faith, and share the unexpected losses.

Of course, in this process, a third party recognized by both parties can also be invited to judge or adjudicate. But no matter what, don't unlock the mortgage data before the final agreement is executed. This is a bargaining chip and a security guarantee. The system cannot determine who has breached the contract. The system only provides both parties with the right to not unlock the other party's mortgage assets so that both parties have bargaining chips. If an agreement cannot be reached in the end, the fisherman contract will confiscate the mortgaged assets of both

parties. The current initial processing of these confiscated assets will be mainly used for public welfare donations for natural disasters, and the original owner of the mortgaged assets can retain the right of signature. Attentive readers must have thought that the ratio of the value of the mortgage asset to the exchange/transaction is the key to safety. This part is discussed in detail in the chapter on security mechanisms.

3.3. Exchange or Trade

The third point, because in the second point, the invitee was invited to lock up his mortgage assets according to the conditions, and both parties were unable to retrieve the assets at this time. This setting is the key to safety. After that, both parties to the transaction/exchange can safely trade/exchange the transaction. Either party can send the exchange first, as long as the two parties implement the agreement and can deliver the exchange to the other party. In order to reduce the loss in the case of default, a "first mover right" is proposed here, that is, the party that promises to send the transaction first and confirms that the other party can pledge less assets than the other party. In this case, the loss is smaller than the peer-to-peer mortgage model in the case of default.

3.4. Unlock Mortgage

The fourth point is that after the transaction is completed and there is no doubt, both parties can proceed with the process of unlocking the collateral. Unlocking can be initiated by either party first. The only thing to note is that unlocking can only be done after both parties have completed the agreed transaction, otherwise there may be losses. After both parties have unlocked their respective assets, the completion of the exchange is marked. When using the system, it is necessary to avoid limitations or misunderstandings in thinking, that is, after locking, both parties can conduct multiple transactions or exchanges. That is to say, the fisherman system is to establish a safe channel, and multiple transactions can be completed through this safe channel.

3.5. Release Mortgage Assets

Point 5, after both parties release the locked assets, the system will release the locked assets of both parties. At this point, both parties can get their assets back.

From the above steps and key points, in the whole process, the system does not touch the user's transaction. This design increases the flexibility of the system, also increases privacy, and has a wider range of applications. After users generate virtual credits through the fisherman system, they can exchange or trade multiple times. It can also be seen from this that the fisherman system is used to provide a security layer and establish a secure channel without restricting the details of the transaction. Maximize flexibility.

4. Security Mechanism

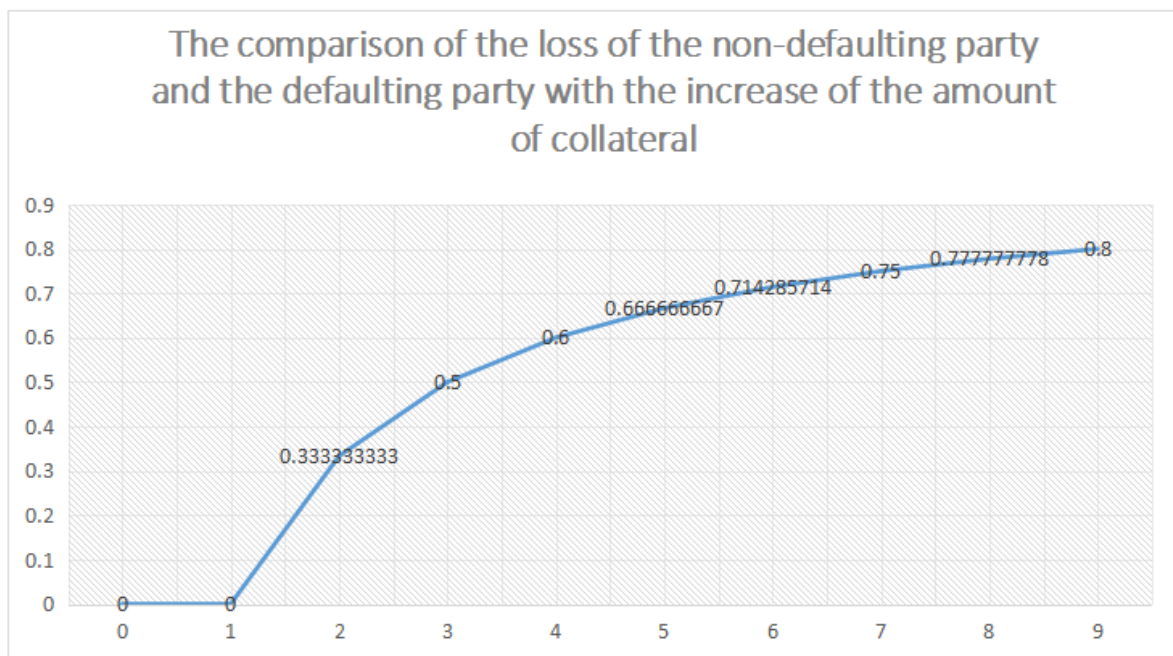
From the introduction in the previous section, we know that the fisherman system ensures that its assets will not be maliciously locked by the conditions specified by the inviter. When unlocking, the mortgage assets can only be retrieved after both parties are satisfied with the transaction result through the "and lock". These two are the hard logic of the fisherman system to ensure transaction security. In fact, it is necessary to cooperate with the setting logic of parameters to ensure the overall safety. Careful thinking people have discovered that the amount of collateral chosen is the ultimate guarantee of safety. If the over-collateralization is unreasonable and cannot have limited expectations for the other party's psychology, it cannot guarantee security.

Here we will carefully analyze the problem, that is, how much the excess amount of collateral should be set to better ensure security.

From the point of view of human nature, normal people are loss averse. If there is a possibility of loss, then the evil behavior will be limited. In addition to this, people will also be affected by the feelings of relative losses, such as self-comforting with the other party's loss more than their own. So when the system parameters are selected, it is very important to strike a balance between these two kinds of psychology. Of course, the system will have enough time for both parties to think calmly and geographically, so loss aversion plays a major role. However, from the perspective of deterrence, emphasizing the psychology of relative loss will also affect the final decision of both parties. The following shows the comparison of the losses of both parties if there is a conflict between the two parties, or if there is a breach of contract.

Collateral/trading multiples	0	1	2	3	4	5	6	7	8	9
Non-compliance party losses	1	2	3	4	5	6	7	8	9	10
defaulting party losses	0	0	1	2	3	4	5	6	7	8
Default/Loss Given Default Ratio	0	0	0.3333333	0.5	0.6	0.66666667	0.71428571	0.75	0.77777778	0.8

Below is a graph of the changes drawn accordingly.



From the figure, we can observe that when a default occurs, as the multiple of the collateral relative to the transaction continues to increase, the losses of the two parties are closer, which also means that the safety factor is higher. The starting point of safety is that the collateral is more than double the value of the transaction. Therefore, in order to achieve the goal of "no loss for defaulters", over-collateralization needs to at least double the value of the transaction.

The Fisherman system does not restrict you to cooperate with other security mechanisms to ensure the security of transactions. When the two sides of the transaction cannot directly negotiate the result, then they can hand over their control to a third party trusted by both parties, who will decide the dispute.

For solving the problem of more loss for the keepers who follow the rules. It should be said that liars should be unwilling to exchange arrogant losses for more losses from others, so liars should leave the system. In addition, there are problems encountered in the transaction process, and the two parties cannot have disputes over who is responsible for these issues, and are unwilling to back down. At this time, the fisherman system will confiscate the collaterals of both parties. A small part of the confiscated collateral will be reserved for the operation of the system, and most

of it will be used for donations to natural disasters, and the original owner of the collateral will retain the right of signature.

5. Roadmap

In the case where support similar to the estimate can be obtained, follow the evolution route as follows.

1. At the end of the first quarter of 2022, realize the MVP (Minimum Viable Product), that is, realize the core function of the system: generate virtual credits. (This part is currently nearing completion)
2. Around the second quarter of 2022, recruit community volunteers to participate in small-scale internal testing of the minimal system. On the other hand, improve other functions, such as invitation and reward mechanism.
3. Around the third and fourth quarters of 2022, establish a community DAO organization to provide a system for everyone.
4. Around the fourth quarter of 2022, develop a system based on telegram bots that traders can use with social tools.
5. In the first quarter of 2023, after evaluating security, fully open source.

6. system economic model

This section describes the sources of revenue for the system and how these revenues are distributed.

6.1 Income and distribution

As an extensible system, the Fisherman system may have the following sources of income:

1. Substantially lock the fees charged.
2. The access service fee when the scalable application is accessed.
3. After the breach of contract, the profit portion of the fisherman will retain the portion of the operating expenses.

These incomes will be shared with system and community builders and participants through a certain mechanism. The distribution mechanism is ultimately formulated by the decentralized DAO.

6.2 Point TOKEN issuance (not yet confirmed)

There is currently no planned release, and the operation of the system does not depend on TOKEN.

Another note: In the later stage, in order to provide the power distribution for building DAO management, and under the feasibility of compliance, points TOKEN will be issued. These points will be distributed free of charge to contributors and participants in the Fisherman community.

7. Reference

[1] [比特币 \(加密数字货币\) 百度百科 \(baidu.com\)](#)

[2] [第三方托管 百度百科 \(baidu.com\)](#)

8. Disclaimer

This white paper is only used to introduce the information of the project system, and it does not constitute investment advice or suggestion. This project does not issue coins, nor does it serve as a transmission medium for transaction transactions. Once you participate in the project, you understand and accept the risk of the project, comply with the laws and regulations of the region where you are located, and are willing to bear all the corresponding consequences. This article represents the current point of view only, and the opinions reflected in this article are subject to change without notice.