Selfcoin

YuBin Wang

Abstract

Selfcoin is the virtual currency system, which is designed by following the economics principle of only labor gains. In Selfcoin the management is personalized that each node just minds it own's business. Thus it is a pure decentralized system without risk of re-centralization. And the cost of system maintain and secure is splited and low. Also, the effect of business network makes the system robust.

Index Terms

Selfcoin, Selfchain, Blockchain.

Selfcoin

I. Introduction

Since the economic system suffers from crisis to this day, it is time to create the new currency system to relieve and even solve this issue. Bitcoin is the first successful and popular virtual currency model to respond. And the followers make remarkable contributions. However, the less attention they pay to the root cause of economic crisis makes them get lost [1]. Thus, most of the virtual currencies just become another tool to speculate and make no difference to the core issue.

Therefore, this paper puts forward a new virtual currency framework called selfcoin, which is designed by following the economics theory of [2]. it aims to overcome the awkward situation of virtual currencies mentioned above, and create a real economically feasible virtual currency to change relations of production, eliminate exploit and economic crisis.

In this paper, Section 2 gives the inspiration of selfcoin, which is a pretty common sense; Section 3 puts forward the selfchain, which is the framework of selfcoin; Section 4 introduces coin generation, which is the core of selfcoin and way to implement economics theory; Section 5 proposes proof of coherent to maintain and secure selfcoin system; Section 6 talks about the robust network topology; Section 7 and 8 discusses privacy and security, separately; Section 9 gives an implementation of selfcoin based on the design mentioned above; The last section concludes the paper.

II. Inspiration

Most of virtual currency systems are designed to have just one unique account, thus just have one chain called blockchain to record the information. In order to maintain this unique blockchain, the cost is huge. Note that like social network, one node only has relations with a fraction of other nodes. The relationship among nodes need only to be maintained by the related nodes. Other nodes are just onlookers. And there is no need at all to bind all nodes together in one chain. Thus, the chain decentralization, which is one chain for one node, can be more flexible.

The inspiration of chain decentralization leads to a series of advantages. First, the node only manages its own chain and maintains its own relations with other nodes, and there is no one big chain that needs all of the nodes cooperate to maintain. Thus there is no meaningless competition for recording rights which causes unnecessary cost, or partial stake which causes re-centralization and monopoly, or massive broadcast which causes Internet congestion. Second, by only taking care of oneself, the cost to take part in this system is affordable for a node, even it is running in the portable devices. Thus there is no concept of full function nodes or simplified nodes.

III. Selfchain

Based on the inspiration of chain decentralization, the paper constructs a new chain structure, which is the base of selfcoin, called selfchain. The selfcoin system is composed by a large number of nodes, each node has its own chain, which is hash linked. A node only records its own activity with other nodes to its own chain. The structure of selfchain is illustrated in Fig. 1. Every chain is leaded by an unique node ID, followed by the indexed recorded activities with other nodes.

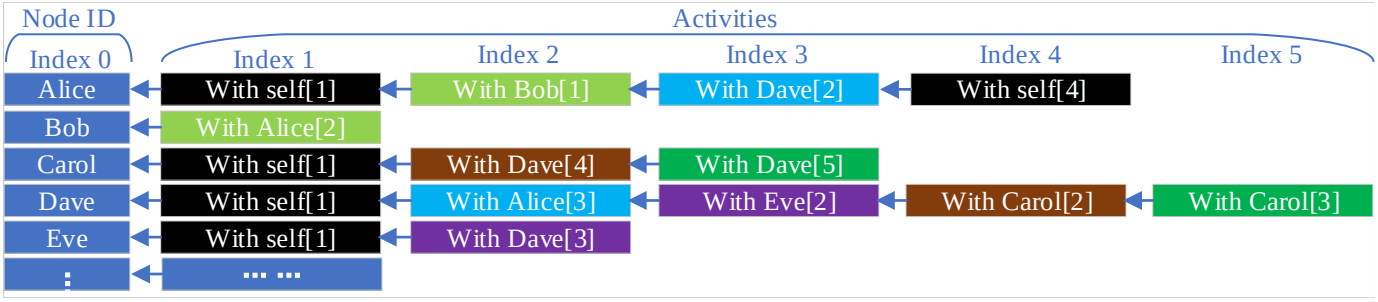

Fig. 1. Selfchain stucture

In the virtual currency system, the node who receives the digital cash has instinct to verify and protect its validity. Logically, each partner has the right and duty to record its own transaction. And since it is totally personal behavior, it is natual to construct the node's own chain by adding the transaction record when trading with other nodes. Thus, selfchain given above is a perfect frame to construct the currency system. And selfcoin system is derived with selfchain as framework.

IV. Coin Generation

For most of the virtual currencies, the rule of coin generation is reckless. Mostly it is restricted by math equation and distributed to system maintainers. However, this paper believes that physical assets and virtual assets which includes minds, ideas and informations, are the source of fortune and should be propagated and awarded directly in the virtual currency system.

In the selfcoin, a unique selfchain, which is managed by a unique node, is created to record the digital assets of every other common node. Since the significance of the unique node, it is named God in this paper. Then every node can add any of digitalized physical assets and virtual assets to God chain by interacting with God. The physical assets, which are easy to be evaluated, can be used to charge for coins. And the virtual assets, which are protected by the chain, can be used to benefit from being the reference. Coins can only be generated based on the charge of physical assets.

V. Proof of Coherent

The way to secure and maintain selfcoin system is Proof of Coherent (POC), which means the selfchain should be linked only one by one without disjointed and branched. If POC of selfchain fails, it means that this selfchain cheats and the related selfchains will suffer. Thus, for the both sides with activities between each other, they have the instinct to verify POC of the other partner constantly to protect their own interests. It is the incentive to protect the whole selfcoin system from malicious nodes.

VI. Network

The network of selfcoin is a bit like social network. Every node only need to verify the POC of the concerned selfchains. And with it the selfcoin system can be robust and secure. Even for a totally strange node, it is completely credible. It is a bit like find a stranger in social network. By just providing the key ID of the stranger, it is easy to find him/her with the help of relations of social network.

In the network, there is one kind of relay nodes to help maintain stability, called Aid. Note that Aid just act as nothing but forwarding and storage nodes. Since usually nodes are handheld terminals like smartphone which is power limited and can be offline voluntary or forced unpredictably, the information can be stored in the Aid and obtained as long as demanded. Also, God node can use Aid to level his tasks and avoid DOS attack.

VII. Privacy

Since the coin generation is related to physical assets, the ID of node in real world needs to be public to be verified. Thus privacy is not part of base framework in selfcoin. However, privacy is a necessary decoration for selfcoin system. Many artful methods are proposed to deal with privacy, like public hash of ID instead of ID until launch initiatively, ID change once public, The Onion Router (TOR), ring signature, zero knowledge and etc.. Privacy can be achieved in defined activities between nodes with additional cost.

VIII. Security

A. Quantum Computing

In the near future, quantum computing can become popular and crack most of the classical encryption algorithms in a very short time. The famous one that can resist quantum computing is hash. And many asymmetric encryptions, like Number Theory Research Unit (NTRU) and McEliece, can also resist quantum computing.

B. Cyber Attack

The most possible and common cyber attack is DOS type attack against public nodes which are God node and Aid nodes. The more Aid nodes, the less suffers from these attacks.

C. Double Spend

Double Spend is prevented by POC.

IX. Implementation

An implementation is given on the base of the selfcoin framework talked above. There are several activities between each node. All of the activities are recorded in the corresponding selfchains, and checked and verified by the relevant nodes. The followings are the detail of each activities.

TABLE I
ELEMENTS

Version	For selfcoin system version control
Time	For time record
Type	The type of activities, like Post, Charge, and etc.
ID	The Public Key of the corresponding node
Mutual Index	The index of transaction between related nodes
Content Hash	The hash of digital substance
Sign	The sign of node who sends card
Hash	The hash of card
Previous Hash	The hash of previous card in the chain
Chain Index	The index of chain of node
Previous Mutual Chain Index	The chain index for previous mutual index
Remained Coin (usual nodes)	The number of coins owned before
Remained Coin (GOD node)	The number of coins charged before
Coin	The number of coins for activity

A. Constitution of activities

These activities are cards which is composed by the following elements illustrated in Table I. Chain Index is used for POC and it demonstrates the validity of the chain. Mutual Index is used to get rid of linkages among nodes in one chain, which means a node can have relations with all of the other nodes concurrently without interaction. Previous Mutual Chain Index is used to track transactions with every nodes.

B. Post Protocol

Post is for publication of physical assets and virtual assets. For doing so, these assets need to be digitalized. The post process is as Fig. 2.

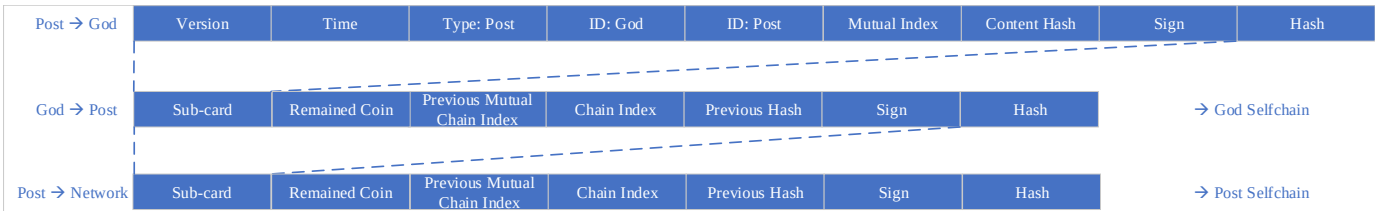

Fig. 2. Post

C. Charge and Redeem Protocol

Charge is for coin generation. Using the digital physical estate posted in God chain, the selfcoin system loans node coins based on market price. When the time is up, the charge estate is redeemed as long as the loaned coins are returned to God. Charge and redeem are illustrated in Fig. 3 and Fig. 4, separately.

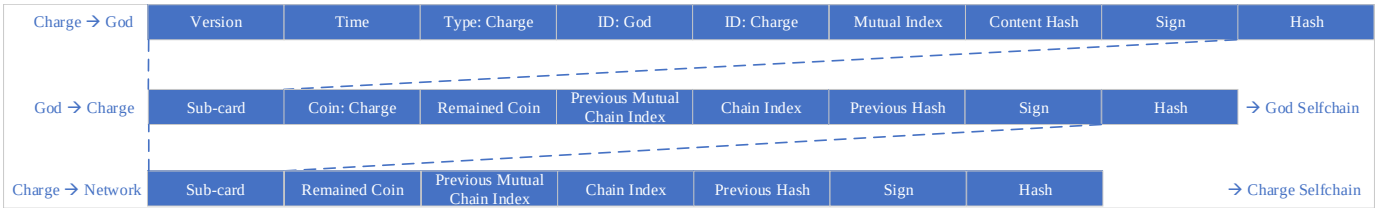

Fig. 3. Charge

D. Trade Protocol

Trade has two cases, one is deferred trade and the other is immediate trade. For immediate trade, payer gives earner pay card directly. While for deferred trade, payer gives pay card to one binding Aid node, and earner demand the card from the Aid node. The immediate trade is shown as Fig. 5. And deferred trade protocol is more or less than immediate trade using demand protocol mentioned below.

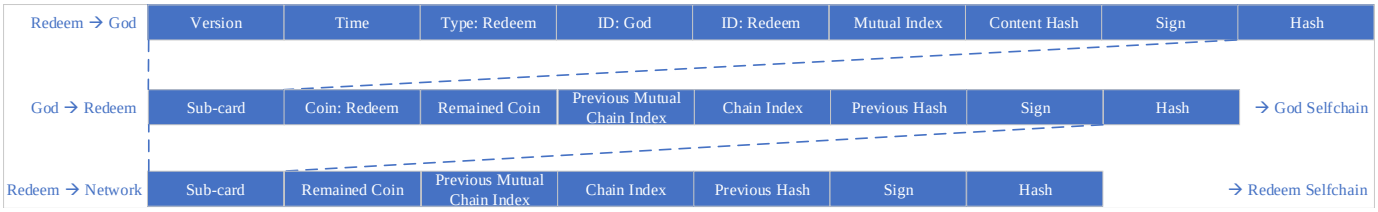

Fig. 4. Redeem

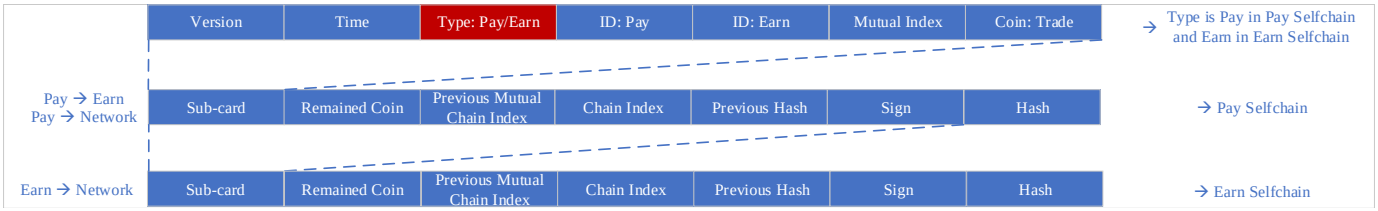

Fig. 5. Trade (immediate)

E. Demand Protocol

Since nodes could be offline and miss card to coherent selfchain, it is common for a node to demand the indicated card from other nodes, more often Aid nodes. Also it is possible that God node demands post and charge cards from Aid nodes. The detail of demand protocol is shown in Fig. 6.

Fig. 6. Demand

F. Watch Protocol

This is the way to verify POC and secure selfcoin system from double spend. For a period of time in the network, some nodes are online, others are offline. Technically speaking, as long as a node is online, it is free to act as a watcher to watch any nodes. Generally speaking, watchers watch their partners to protect own interests. If watcher finds that the card information is invalid, it will alarm the whole system with evidence and the malicious node will be confirmed and bannished.

X. Conclusion

The main idea of the paper is to build a virtual currency system, selfcoin, to let wealth creator be wealth taker in feasible way. With the proposition of chain decentralization, the design of selfcoin takes economics as cornerstone in coin generation, and puts forward POC to maintain and secure the whole system efficiently by using the network topology to enhance robust. The paper thinks privacy is not compatible with coin generation, so it is not integated into framework design of selfcoin, but can be decorated on the system by choosing suitable up-to-date innovation about privacy protection. And the low cost of selfcoin enable it to run in mobile devices. Hopefully, selfcoin can make the life free, fair and efficient.

References

[1] Y. B. Wang, “Ponder of virtual currency.”
[2] ——, “Blueprint of currency economics.”