Ponder of Virtual Currency

YuBin Wang

Abstract

This paper summarize pros and cons of the existing virtual currency, including Bitcoin, Ethereum, Monero and etc.. Then analyses the lost of these coins, which gives the answer to why these coins are nothing but the tool for speculation and impractical in economy. And points out the right purpose to design virtual currency that satisfies principles of economics and social humanity.

Index Terms

Virtual Currency, Bitcoin, Ethereum, Monero, Zcash, Byteball, Unit-e.

Ponder of Virtual Currency

I. Introduction

For centuries, the currency plays an important part to make our lives better. The rise of productivity is based on social division of labour. It is a wonder that an individual can get anything wanted from the community by focus on one experted territory. But also for centuries, the currency is abused by ruling class and interest group to act as an efficient tool to exploit hard workers. To fight back, the first and important step is to design a new currency with the consensus of the spirit of liberty and equality.

Firstly, this paper analyzes the existing virtual currencies and points out the drawback. Then the purpose to design virtual currency is put forward, which overcomes the awkward situation mentioned in the two sections above. The main idea of this paper is trying to give a proper framework for virtual currency, which can be applied in the economic system to change the relations of production.

II. Existing Virtual Currency

A. Bitcoin

Bitcoin [1] is the milestone for virtual currency history. It brings impact on people's both life and mind. The folloing talks about every aspect of Bitcoin.

1) Proof of Work (POW): Using POW, Bitcoin wants to create a decentralized system. It thinks that for a node, it is nearly impossible to own more than half of all involved compute power, thus centralization is borken. However, this illusion has already been overthrown by reality. The mining pools are formed and become larger and larger. As the matter of fact, it is impossible to create a decentralized system by competition. Winner takes all.

2) Cost: Using POW, the cost of competition can not be neglected.

3) Inspiration: The inspiration is also the generation of bitcoins. While it can sustain the whole system by inspiring miner, is it reasonable for the society and economy? Currency is the symble of fortune, it should be owned by fortune maker, not the currency maker. And even more, there is no valid mechanism that makes correspondance between the sum of coins and the sum of social fortune.

4) Privacy: Bitcoin values privacy and protects privacy by separation the ID of real and virtual. Some reaseach indicates that it is not so convicing.

Summing up, Bitcoin has flaws everywhere. The crucial point is that its design priciple does not follow economics. There is no wonder that it ends up as the tool of speculate.

B. Ethereum

Ethereum [2] is the platform on which runs decentralized applications with blockchain technology. Basically, the design principle of this decentralized system is the same as Bitcoin. The improvement is that its application is not limited in financial, but any other decentralized territories.

C. Monero

The major contributions of Monero [3] are promoting the privacy and POW compared with Bitcoin. For privacy, Monero uses one-time ring signatures to achieve untraceability and unlinkability. For POW, Monero claims that it uses a more egalitarian POW which is a new memory-bound algorithm.

D. Zcash

The most highlight of Zcash [4] is that it applies cutting-edge to achieve solid anonymous based on Bitcoin, which is different from Monero's and called zero-knowledge succinct non-interactive arguments of knowledge (zk-SNARK). And inevitably, it is more complex and costs more sources.

E. Byteball and IOTA

Byteball [5] and IOTA [6] use Directed Acyclic Graph (DAG) as the framework instead of blockchain. DAG is the tangle of multiple chains.

F. Burst and BHD

Burst [7] and BHD [8] use Proof of Capacity (POC) as consensus. POC uses tiny low power compared with POW, even though it is run at the cost of capacity.

G. PPCoin

Proof of Stake (POS) is used as consensus in PPcoin [9]. POS has the risk that rich get richer, which is the anti-decentralized against blockchain.

H. Unit-e

Unit-e [10] is an updated cryptocurrency invented by the distributed technology research foundation (DTR). It includes a series of improvements of virtual currency system. Notably, it takes economics as a central and open question in the design of Unit-e, and tries to design a more rational mechanism to incentivize players and sustain the whole system.

III. Lost of Existing Virtual Currency

Since the born of Bitcoin, dozens and hundreds of virtual currencies have been promoted in public. Though, more or less, they indeed propose many valuable methods to push the territory of virtual currency to move forward, however, the key issue, which is how to integrate into economic system to make it healthy, remains untouched. And frustratingly, most of these currencies are used as speculation instead of real exchange for mutual economic benefit.

During the last ten years, the rapid growth of virtual currency brings a lot progresses in technology: POC and POS for lower power; zk-SNARK and ring signature for privacy; DAG for rapid trasaction; and so on. But when it comes to coin generation and allocation, most of them attempt to achieve it perfectly by using some simple math functions and equations, which is naive for economic. The paper believes that the principle of economics is far beyond than that. Economic phenomenon is intricate and variable in real word. And currency plays an important role in it. Thus in the design of every currency, economics is the core. The territory of virtual currency has lost for a decade by neglecting coin generation and allocation, by being used as speculation to chase interests, and by failing to function as currency for real exchange in real world.

Since the deficiency of legal currency, which fails to make economy operate properly, the new currency is needed to take the place and it should be just, efficient and feasible. The following section gives the purpose to design such potential virtual currency.

IV. Purpose to Design Virtual Currency

A. Decentralization

Since competition and vote are not the right ways to achieve decentralization, some traditional thoughs need to be broken. Satoshi Nakamoto claims that, quote as, what is needed is an electronic payment system based on cryptographic proof instead of trust. For now we proved that the virtual currencies listed above all fail to decentralize using cryptographic method. This paper does not say that it is impossible for society to discard credit. It doubts the possibility to achieve this in near future, and tries to find a workaround.

Speaking of credit, people are not worried about it. people loan money from bank with their property credit and even just ID credit. Credit is worth and people can not afford to lose it. What people worried about is centralized credit, like legal currency system. Credit decentralization can be a better choice when design virtual system.

B. Coin Generation

The way of coin generation is the way to deal with property. A reasonable and practical virtual currency system should satisfy the right theory of economics. Note that if it flatters wrong economic claims, there is no way to eliminate the brought crisis since the decentralized system is much harder to control compared with legal currency. This paper recommends theory of economics cited as [11]. For coin generation, the mian idea is that it should be in accordance with real social property. The teconology of digitalization of property can help to achieve this goal.

C. Privacy

For economic system, it is known that open and free are main theme. But privacy should be taken into consideration. So the recommend is that public is foundation stone and privacy is necessary decorate.

V. Conclusion

It is necessary for Bitcoin and its followers to devote themselves to decentralization of financial system to avoid economic crisis. But that is not enough. The root cause of the crisis is exploit. And any virtual currency which overlooks this root cause leads to nothing changed inside. Thus, find a proper way to guide the design of virtual currency is important and urgent. Combining with the technology of Bitcoin and its followers, it is believed that an innovated virtual currency will emerge in the public.

REFERENCES

[1] Std. [Online]. Available: https://bitcoin.org/
[2] Std. [Online]. Available: https://www.ethereum.org/
[3] Std. [Online]. Available: https://monero.org/
[4] Std. [Online]. Available: https://z.cash/
[5] Std. [Online]. Available: https://obyte.org/
[6] Std. [Online]. Available: https://www.iota.org/
[7] Std. [Online]. Available: https://www.burst-coin.org/
[8] Std. [Online]. Available: https://btchd.org/
[9] Std. [Online]. Available: https://peercoin.net/
[10] Std. [Online]. Available: https://dtr.org/
[11] Y. B. Wang, "Blueprint of currency economics."