Properties of an Ideal P2P Monetary System and LibreFortune

LibreSeed Inc.

June 09, 2014

Abstract

In this paper, We explore some desired properties that an ideal P2P monetary system should have. We summarize important principles and common pitfalls in designing a P2P monetary system with examples. Being aware of all the difficulties and pitfalls discussed in this paper, we designed LibreFortune — a new P2P currency with security, fairness and sustainability as primary designing goals. A brief introduction to LibreFortune is given at the end.

[Paste to Microsoft Word for syntax check.]

1 Introduction

Ever since Satoshi Nakamoto introduced *Bitcoin* in 2009 [1, 2], it gained an increasing interest. Bitcoin's lasting popularity over the recent couple years has proven that it is a well-designed system. However, as we began understanding more about the system, we realized that it had some drawbacks that prohibited it from growing to a sustainable monetary system, notably the energy waste being too high.

However energy-consuming has fundamental meaning to the security of *Proof-of-Work* (PoW) [3] framework (which Bitcoin falls in). Resolving such an inherent issue is far beyond small tweaks. Discussions of using *Proof-of-Stake* (PoS) [4], as an alternative to PoW, to design monetary system had been around as early as 2011. The idea of PoS is simple and appealing. But in contrast to PoW, provable security in PoS framework is much more difficult to achieve. Designing a concrete PoS system that is secure against various attacks requires much more than the basic idea "Proof-of-Stake".

Due to the rise in popularity in Bitcoin, many have introduced their very own digital currency systems in attempt to rival or improve Bitcoin. However new features and tweaks can easily introduce new vulnerabilities, especially when their implications on security are not throughly examined.

As more and more new digital currency systems come to being, it is time for us to think – for an ideal P2P monetary system, what properties must it have, what issues must it avoid, and what common attacks does it face to? In this paper we discuss these questions in general with examples. Note that we are not trying to exhaustively list out all the properties of an ideal P2P monetary system. This paper just summarizes some important principles of designing a P2P currency in the hope of being helpful to other P2P currency designers in examining and improving their designs.

Finally, Section 3 briefly introduces *LibreFortune* — a new P2P monetary system. We designed it bearing in mind with all the properties, issues and common attack strategies discussed in this paper.

The following discussion assumes that the reader has been familiar with how digital currencies work, as well as the concepts of Proof-of-Work and Proof-of-Stake. If not, we encourage the reader to first read the resources in References.

2 Ideal P2P Monetary System

This section will discuss three topics: security, fairness, and a closed system. For each topic, we will elaborate on why we think it is important, and relevant examples to demonstrate our thinking. Although most examples are about well known PoW and PoS frameworks, the principles should have general applicability.

2.1 Security

An ideal P2P currency system should be safe when honest users control more than 50% of the resources. Specifically, the probability of successfully pulling off an attack should rapidly decay to zero as the resources controlled by the attacker goes down below 50%. The high rate of decay should be mathematically provable.

A P2P system does not, and should not have a central authority, thereby, making it if at any time there are conflicting chains, the side occupying more resources will decide which is the main chain. Because of this, if a user party hold more than 50% of the resources, inevitably it will then be able to hold control over the system. The problem of a single party holding more than 50% resources is called *The Monopoly Problem*[5]. Due to fairness of the system to all users, it is impossible for the system to deny a potential attacker from holding more than 50% of the resources. But in an ideal monetary system, the incentive for a large resource holder to launch an attack should be minimal.

What a good design can guarantee is reliable system safety under a no monopoly circumstance. In this respect, Proof-of-Work systems can achieve that straightforwardly at the cost of using substantial resources like electricity. But to Proof-of-Stake systems, it is of a much more serious challenge. Designers of Proof-of-Stake systems need to deeply consider a few questions to avoid hidden vulnerabilities:

1. Could the resource for block generation (mining) be accumulated over time?

   If so, an attacker with minor resources would be able to generate many blocks into the system at once as long as they have waited for a sufficiently long time, which might result in a large main chain switch. The attacker can easily associate double-spending attack with the malicious main chain switch. Coin-age based system is a typical category that is susceptible to this kind of attack.

2. Is it possible for an attacker to establish additional advantage in generating a later block by making early setup?

   In a very simple form, is it possible for the generator of block n to make some favorable adjustments when generating block n, such as reorganizing the stakes at hand or inserting a particular transaction, in order to gain advantage in competing for generating block $n+1$? Note that the generator may have multiple accounts, thus the beneficiary may be an account other than the one generating block n.

3. Does one with $k\%$ of the resources has probability of $k\%$ to generate the next block in the main chain?

   In practice, it is hard to make it strictly $k\%$, but should be within a negligible range. Otherwise, for a fixed total amount of resources, splitting or merging it will affect its overall efficiency in block generation. If that is the case, an attacker with less than 50% resources may beat the main chain by optimizing the configuration of his or her resources, which means the resource threshold of pulling off an attack is below 50%.

   In terms of fairness, one can also argue that it is unfair if a 2% stakeholder can generate more than twice as many blocks as a 1% stakeholder.

4. If node A is the first to generate block n, do all other nodes abandon their current work on block n, accept node A's block n and then proceed onto block $n+1$?

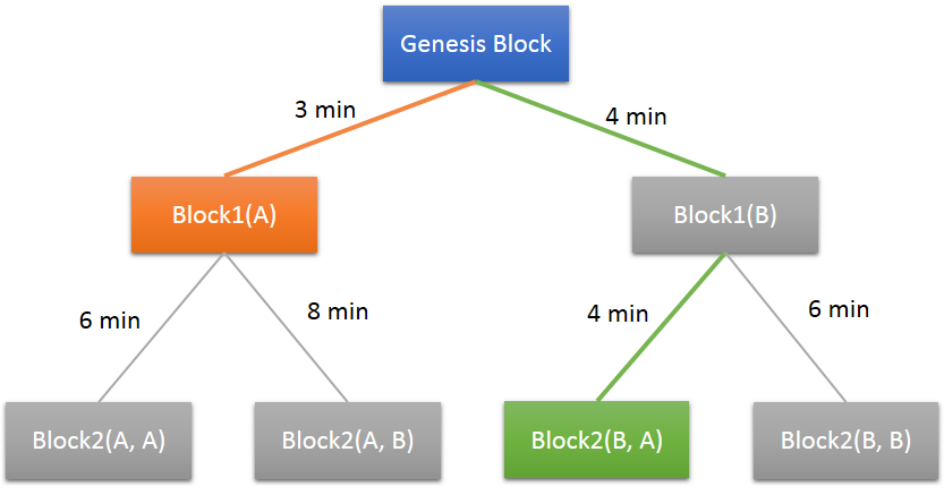

Figure 1: Example - the earliest block at height two is not originated from the earliest block at height one.

Consider an example shown in Figure 1, the earliest block at height one is *Block1*(A), which will become the main chain of length one. But the earliest block at height two *Block2*(B, A) is originated from *Block1*(B). Thus if the miners are willing to give a shot on the suboptimal block *Block1*(B), block *Block1*(A) will be switched out of the main chain later on.

In a Bitcoin-like PoW system, mining on a suboptimal branch is as costly as mining on the main chain. Thus normally it only make sense to exclusively mine on the main chain. But in a PoS system, mining on a block branch usually requires only minimal cost. Thus a node will be able to mine on many branches (including the current main chain) at the same time, making the strategy of searching optimal branch in the above example viable. Actually, the effect of this strategy can be significant. In a simulation, we observed that a group of miners can achieve 1.7x boost in mining efficiency by employing a branch searching strategy.

Besides block chain protocol, deep consideration should be also given to safety issues in other parts, e.g. wallet, network, etc.

2.2 Fairness

In mining, fairness mainly refers to that the efficiency of mining should be proportional to the amount of resources of the miner. A miner should be able to freely organize the resources at hand without affecting the overall mining efficiency. This is an important principle to follow, because not only it conform with people's intuition, but also it has important security implication (as explained in Section 2.1). In the PoS context, fairness also means that if a miner possessed a stake for d days and then sold it out, this miner should have the right to mine with the stake for exactly d days. In this sense, in a PoS system making use of coin-age as mining resource, resetting the coin-age to zero when a coin is spent might be a potential unfair design that need to be carefully examined.

In the Main Chain Protocol (i.e. the rule of determine which branch is the main chain), fairness means that for any two branches, there is a fair and objective solution to determine which is the better branch. In the P2P monetary system, any node, any block, any user should be treated equally. The Main Chain Protocol should avoid including rules of artificially marking a block or a miner as abnormal or malicious (via

voting or other mechanisms). Anyway, such rules will not help when two conflicting branches marking each other as abnormal.

2.3 Closed

Closed means that the operation of the system is not reliant on any external resources. It is highly desired to the sustainability of a system. Otherwise, once the resource is not sufficiently available, or when there is a conflict of interest, the system would be at risk.

In PoW systems, take Bitcoin for an example, the system security is essentially hinged to the rate of ongoing large power consumption via ASICs, thus it is not closed. Because the total award of mining is fixed and is distributed to the minors in proportion to their computing power, there is an endless "Mining Arms Race" among all miners. As the race became more and more intensive, the rate of return continuously went down. In the future, two possible results of this are: 1) many miners will stop mining because they can no longer profit; 2) users will be charged high transaction fees to sustain the cost of mining. The former will threaten the security of the system, while the latter will limit the usability of the system in, for example, small payment.

A well-designed PoS system can be closed in that the mining process can rely only on internal resources, i.e. the currency of the system. The users only need to hold currency, i.e. stake, to participate mining. No ASIC needed, no constantly high rate of power consumption required. Because the miners are the users, it is simple to come to a consensus on a fair rate of transaction fees. This is a merit of PoS systems for being closed — all the profit is relevant to the same group of people. This is not the case in Proof-of-Work systems where users favor low transaction fees, while miners favor high. Furthermore, if there is a issue need to be resolved by voting, presume that the voting is associated with block generation, the voters are exactly the stakeholders — the beneficiaries of healthy development of the system.

3 LibreFortune

LibreFortune is a P2P crypto-currency, which is based on Proof-of-Fortune concept (our implementation of Proof-of-Stake). The core idea of LibreFortune was sparked out in early 2013. After numerous rounds of refinement, the design finally completed in late 2013. During the whole designing process, the team played a role more of an attacker

than a developer. When a new attack strategy was found, we never tackle it by directly patching — what interested us was the flaw in the philosophy of the design revealed by it.

We believe that P2P currency is still in its very early stage. Security and sustainability are still the primary goals to achieve. Being a serious attempt to that, the design of LibreFortune follows all the principles discussed above.[1]

Besides, LibreFortune also has the following features:

- Fully decentralized. In LibreFortune, we even do not need a checkpoint to speed up the download. We achieve the same purpose via a structure called skipback-list, on which one can trace back from block n to any previous block within $O(\log n)$ jumps.
- While mining, the wallet can keep encrypted. (This should be a first in Proof-of-Stake systems)
- The payment system is more powerful, secure, and intuitive. Our payment modes support useful parameters (e.g. deadline, weight, etc) so that users can more easily achieve important trading patterns.
- Safe and convenient pooled mining. Users do not need to transfer their coins into the pool to join pooled mining.
- The system is upgradable. We will try our best for the release, inevitably upgrades will be required later. Our protocol has good extensibility, so new features can be introduced in the future when needed.

The basic setting of LibreFortune:

- Green mining.
- Blocks are generated every 4 minutes on average.
- The Genesis block issues 1,312,500 coins.

[1]For one exception, the ideal property "a miner with $k\%$ of the resources has probability of $k\%$ to generate the next block in the main chain" (see Section 2.1) is not perfectly achieved. If a stake is split into small parts, its mining efficiency will slightly decrease. (Consider a very bad case: if a stake as large as 33% of the total stakes is evenly split up into infinitesimal pieces, its mining efficiency will decrease by 0.07%). In practice, this difference is negligible comparing to other influences, e.g. network condition.

- After the Genesis block, every block mints 20 coins, and this amount halves every 4 years.
- The total amount of coins is 21, 000, 000, the same as Bitcoin.
- The currency supports up to 10 decimal places.

4 Acknowledgements

We would like to express our appreciation to Bitcoin, which brought us with the new territory of decentralized currency. We would also like to thank the original idea of Proof-of-Stake — indeed, our work is finding a right way to implement it.

References

[1] "Bitcoin: A Peer-to-Peer Electronic Cash System."
https://bitcoin.org/bitcoin.pdf.

[2] "Introduction to Bitcoin."
https://en.bitcoin.it/wiki/Introduction.

[3] "Proof of Work."
https://en.bitcoin.it/wiki/Proof_of_Work.

[4] "Proof of Stake."
https://en.bitcoin.it/wiki/Proof_of_Stake.

[5] "Motivation For Proof of Stake."
https://en.bitcoin.it/wiki/Proof_of_Stake#The_Monopoly_Problem.