Evolution of Energy-Free Consensus: From POS to SPOS

Team of Project VEE

September 17, 2018

Abstract

A performance-oriented proof-of-stake consensus called Supernode Proof-of-Stake Consensus with the features of constant interval block [illegible]ld minting and stake liquidity has been designed for the VEE blockchain platform. We a[illegible]e the lineage and differences to the original Proof-of-Stake Consensus introduced by Peercoin in 2012.

1 The Role of Energy

Back in 2011, Bitcoin network experienced probably its first phenomenal growth. The energy consumption of the decentralized network was probably not a concern to most of its users and proponents. Yet, Project Peercoin[1] already raised the question that, was the energy consumption really essential in achieving the consensus? To most Bitcoin advocates, the answer was yes. Bitcoin is like gold, the energy consumed in mining gold gives it value, while the energy consumed in mining Bitcoin not only achieves and secures the consensus, but also backs Bitcoin's monetary value.

But historically, opinions vary greatly on what really gives gold monetary value. The Austrian School speculated that it must arise from an initial commodity value[2]. Some speculated that gold should have little value, once nation states are powerful enough to strip gold of its monetary roles. Once one believes in Bitcoin's monetary utility, natually, one would ask what gives Bitcoin value?

In some sense Peercoin took the adventure in solving this central monetary mystery. Peercoin managed to separate the energy consuming component known as proof-of-work - or mining, borrowed from the analogy of gold mining - from the consensus algorithm, and limited energy's role to issuance only. It is then very easy to test energy's remaining link to issuance, as it is trivial to remove the energy component from the issuance mechanism by switching to a stock-like issuance model.

So indeed, proof-of-stake consensus technology further demonstrated that monetary value does not derive from energy consumption. Nor does it require intrinsic value, or any other commodity value. Monetary utility alone could give value.

2 Proof-of-Stake Consensus - The Energy Free Consensus

Peercoin's approach to consensus was quite pioneering. It abandons the amazingly succ f-of-work consensus of Bitcoin entirely, in search of an algorithm that has absolutely no depend ergy consumption at all. It puts a lot of faith into proof-of-stake, believing that the concept could stand alone to form a consensus algorithm, not requiring any proof-of-work component whatsoever. Some authors misunderstand this point. In terms of consensus algorithm Peercoin is pure proof-of-stake. Proof-of-work was only used for fair distribution of coins, without participation in consensus algorithm.

In an energy free consensus system, we refer to the process of block generation as *minting*, in contrast to the energy intensive process of mining.

Peercoin's consensus algorithm inherits some of the features of Bitcoin. For example, it also generates block in a random process, only an average block interval or a target block interval can be observed. Associated with the process is a measure called proof-of-stake difficulty, with which an adjustable threshold is maintained in the consensus protocol for minting of blocks.

The introduction of proof-of-stake consensus is a major milestone in the development of blockchain technology. It not only eliminated the cost associated with mining in order to form distributed consensus, but also greatly expanded blockchain's ability to scale-out, paving the future for diverse applications of the technology.

3 Criticism of Proof-of-Stake Consensus

Since Peercoin's ground-breaking work, some oftenly criticize aspects of the system. One often-heard criticism is known as stake grinding. This attack was discovered in 2012 shortly after Peercoin's initial release[3]. An important new algorithm was implemented in the 0.3 release of Peercoin[4] in February 2013, in defense against this type of attack.

The updated algorithm introduced a consensus field called *kernel*. It is a consensus number that is slowly evolving with the blockchain, where for a given period one block is chosen by the protocol such that the chosen block may contribute one bit of change to the kernel. The kernel may be considered as a slow changing entropy source on the blockchain that a short length of blockchain fork may only impose very limited effect. With the protection of kernel, the threat of stake grinding is generally eliminated.

Another common criticism on proof-of-stake consensus is known as the nothing-at-stake problem. The argument goes, since minting involves no work or energy consumption, the minter loses nothing when attempting to mint on all branches of the block tree. Therefore the minter will have incentive to mint on all branches to avoid the loss incurred when a given fork loses in the competition. The problem with this argument is that it ignores the core tenet of proof-of-stake. The idea of proof-of-stake is, as one owns a portion of stake in the coin supply, one should already have incentive to do good for the whole

system, and disincentive to attack the system. Since minting on all branches is considered as an attack on the protocol, it is already discouraged through proof-of-stake. Under this view, even the so-called rational minter should not measure value in terms of the built-in currency unit, but rather consider the total value of one's own stake measured by an external stable currency.

Considering the potential negative impact on one's stake value, this may be related to the tragedy of the commons[5]. However even under the original interpretation of the tragedy, the potential to avoid a few minting loss could not compare to the magnitude of potential loss in stake value. In practice, nothing-at-stake has not shown to be warranting any protocol adjustment for further deterrence.

4 The Debate of Cold Minting

Shortly after the birth of proof-of-stake consensus, the Peercoin community engaged in a discussion as to the feature of *cold minting*[6][7][8]. This is related to the Bitcoin feature called cold storage, that is, private keys are managed in offline wallets. Because proof-of-stake consensus requires minter to sign the block, the minter's private key must stay online for the task, which is in conflict with the high secuity available to cold storage.

The solution is to separate the role of minting and spending. That is, the key owning the stake can be different from the key doing the minting. Then, while the minting key stays online, the ownership key can be put to offline storage.

This would naturally allow the possibility of minting pools, bearing resemblance to the mining pools of Bitcoin. Given the history of centralization tendency of Bitcoin mining pools, it certainly can be an argument disfavoring such practice.

Due to many reasons, the cold minting feature hasn't been implemented in Peercoin. The separation of minting key and ownership key has since been implemented in several other proof-of-stake systems. It is now commonly referred to as delegation or lease.

5 The Shift Toward Supernode

In the last couple years the blockchain industry has seen tremendous growth in decentralized applications. Both Bitcoin and Ethereum have experienced periodic congestions. More and more focus has been put on single chain performance.

This has raised several issues with respect to consensus algorithm designs. First, mining/minting nodes might not have enough incentive to upgrade the hardware of the nodes. There can also be a great number of such nodes. Some of the nodes are bound to lag behind with hardware upgrade in such situation, as the total maintenance cost in the whole network can be quite significant.

Another issue is related to the random process of block generation in Bitcoin. Although the average block interval is 10 minutes, sometimes one needs to wait much longer for the next block. This is an issue in a performance oriented system. The response of the system is preferred to be constant rather than randomly distributed.

These considerations strongly calls for a constant block interval minting design where the minting nodes are elevated to a more significant standing than other nodes in the network.

6 Minting Slot and Minting Right Contention

In order to achieve constant block interval minting, we define a certain entity called *minting slot*. Each slot corresponds to an equal share of minting right. Thus for a potential minting participant, one must acquire the ownership of a slot in order to obtain the minting right.

There are 60 minting slots defined, each corresponding to a specific second within the minute. To have the minting right at a given second, one must own the corresponding minting slot at the second.

Essentially minters would take turns to mint in this system. The advantage is, should some of the supernodes stop minting for whatever reason, the impact to both [illegible]sponse and throughput is minimized.

The local clock of each supernode is synchronized through network time protocol, to ensure the proper ordering of minting events. Back in 2009, Bitcoin chose not to depend on network time protocol for clock synchronization, so Bitcoin protocol could forgive a miner with clock-skew up to 2 hours. Generally speaking network time protocol nowadays can be regarded as essential Internet services like domain name service, so it can be reasonably assumed a high level of security.

Contention of minting slot is allowed to occur freely at any time, by a challenger to the current minter on a slot chosen by the challenger. There is a relatively high contention fee as a deterrence to abuse. When a challenger issues a contention transaction, the stakes of both contender's and current minter's stakes are examined by the protocol to determine the winner of the contention.

7 Economy of Minting

The stake that participates in minting includes the coins owned and not leased out by the minter, as well as the coins leased by other users to the minter. The term lease refers to the relation that minter typically acts as a minting pool and is expected to pay some interest back to the owner of the coins. The ownership of the coins is never transferred in the lease relation, so there is no way for the minter to spend or transfer the leased coin.

Equal minting right of the minting slots gives the supernodes equal standing and minting output in the network. This is in contrast to Bitcoin's mining design where there is no built-in mechanism to deter

the formation of monopoly in the mining pool market, which has been shown to be a practical threat to the decentralization goal of the system.

The equal minting right of minting slot serves an essential role in the economy of minting. Supernodes form a market of minting pools. The minting market will then form an interest rate for leasing. Since stake owners have a reasonable preference to lease to a supernode paying higher lease rate, and the additional lease to a high paying supernode will lower its lease rate due to the constant minting output of the supernode, an equilibrium exists as a built-in force to equalize the lease rates of supernodes.

The fee destruction model of Peercoin has also been adopted to serve the purpose of lowering inflation while eliminating the conflict of interest between minters.

The hardware resource requirement of supernode is standardized and promoted through community effort outside the scope of the consensus protocol.

8 Stake Liquidity and Busy Contention Attack

Previous proof-of-stake consensus systems placed various restrictions on the movement of stake once it participated in minting. Although technically it may be of good reasons, economically it is a barrier of entry for users to participate in minting.

However, in proof-of-stake consensus, the amount of stake participating in minting is directly related to the security level of the consensus. In this sense it is beneficial for the security of the network if there is no restriction placed on the movement of stake. We call this feature *stake liquidity*. With stake liquidity guaranteed, the minter can spend or transfer the owned stake at any time. The owner of leased stake can cancel the lease relation and spend or transfer the stake at any time as well.

The guarantee of stake liquidity has introduced possibility of certain attacks. From the point of view of proof-of-stake, one should not be able to use the same stake to claim minting right on multiple minting slots. However since the stake is liquid, one might be able to take advantage of the liquidity and attempt to quickly move the stake around to claim more minting slots than it should. We call this type of attack the *busy contention attack*.

The way to defend against this type of attacks is to introduce a measure of the account balance like an accumulating average for the contention of minting slot. The idea is that the stake must stay for a while in the account for the balance measure to increase to the full amount, thus thwarting the busy contention attack.

9 Account Model and Balance

Traditional accounting systems use an account model, where a changing state called balance is precisely tracked together with transaction history.

Bitcoin internally uses a different representation that we call the coinbag model. In order to obtain the account balance, one must collect information about the coinbags associated with the account or address, and add up the amount in each bag to get the balance.

In the last couple years many cryptocurrency systems have returned to the more traditional account model. VEE also adopts the account model where balance can be more efficiently tracked.

With the relation of lease defined, the basic balance of each account can be described from two different parts: the regular balance, which is the owned balance, and the *minting balance*, which is the regular balance plus any received leases, then minus any coins one has leased out. These two different types of balance will be changed immediately when any balance related transaction is confirmed.

10 Proposed Balance Scheme

10.1 Coin age

Coin age is defined as currency amount times holding period. For example, coin age in the unit of coin-day is a number derived from the product of the number of coins multiplied by the number of days the coins have been held.

Just use the same exam Peercoin paper, if Bob received 10 coins from Alice and held it for 90 days, we say that Bo mulated 900 coin-days of coin age. Additionally, when Bob spent the 10 coins he received from Alice, we say the coin age Bob accumulated with these 10 coins had been consumed (or destroyed).

As a proof of value to control the probability of minting a block, coin age shows its advantage and stability. However, since it is transaction based value, the calculation complexity is related to the number of transaction executed during the period. Moreover, it is still not an accurate value to represent the minter's contribution to the community.

10.2 Confirmed balance

Confirmed balance is minting balance (total regular balance + leased in - leased out) confirmed after N blocks.

$$C_n = \min\{B_n, B_{n-1}, \cdots, B_{n-N}\}, \tag{1}$$

where B_i is the minting balance at Block/height i. N is a consta to estimate the effective interval.

The advantages of confirmed balance are

- balance can not increase immediately by some large inputs but can immediately decrease after a large transfer out;
- in order to reach a high confirmed balance, miners/minters need to collect and keep the coin for a long period.

However, it still has its own disadvantages.

- A continuous/cumulative input will not affect the calculation in this period;
- The calculation complexity is $O(N)$. In high minting speed case, in order to reach a better performance and higher stability, a larger N needs to be chosen. In this case the $O(N)$ algorithm will be an issue to affect the system performance.

10.3 Proposed balance calculation scheme

10.3.1 Weighted average balance

In order to avoid the disadvantages of the confirmed balance and reduce the calculation complexity, a new balance with more properties and easier to calculate needs to be designed in high mining/minting speed blockchain system.

Borrowing from the idea of load average in operating system and stochastic process formula, we designed following weighted average balance first,

$$W_{h_n} = \alpha B_{h_n} + (1-\alpha)W_{h_{n-1}}, \tag{2}$$

where

$$\alpha = \begin{cases} \frac{h_n - h_{n-1}}{N}, & \text{if } h_n - h_{n-1} < N \\ 1 & \text{otherwise} \end{cases},$$

h_n is the height of current block, and h_{n-1} is the height of the last block where the account minting balance changes.

The calculation complexity of this new designed balance is reduced to $O(1)$ with weighted average balance recorded after every minting balance changing. And its max increasing speed is linear (see Example 11.1). However, from Example 11.1.1 and 11.1.2, we can find the decreasing speed of weighted average balance is slow if the balance changes frequently. Additionally, it is a good property if the total weighted average balance is controlled. This means that the balance will not be created with unfounded source (similar as energy conservation law in Physics). From Example 11.2.1 and 11.2.2, we can conclude that the weighted average balance formula does not follow the conservation law.

10.3.2 Minting average balance

In order to keep the good properties of weighted average balance and overcome the disadvantages, we proposed a new balance called minting average balance (MAB) as follows:

$$S_{h_n} = \min\{B_{h_n}, \alpha B_{h_{n-1}} + (1-\alpha) S_{h_{n-1}}\}, \tag{3}$$

where B_{h_n} represents the current balance at height h_n.

Minting average balance takes the minimum of the current balance and weighted average balance. The calculation complexity is still $O(1)$. Moreover, in this formula, MAB will decrease directly to 0 if one transfers all his/her balance out. With this property, total minting average balance will be conservative and controlled by total balance.

11 Examples

In this section, we will design many numerical examples to show the properties of minting average balance. Assume the minting speed is one block per second, then we will collect $24 \times 60 \times 60 = 86400$ blocks in one day. In this section, we will set $N = 86400$ for **all** examples. And we also set all transaction fee equal to **zero** as ideal cases.

11.1 Increasing and decreasing speed

The first example in this section is about the increasing and decreasing speed.

11.1.1 Simple increasing and decreasing speed

Alice and Bob both have initial balance equal to zero. Alice will receive 1 coin per block and Bob will receive 86400 coins at height 43200. The increasing performance of Alice can be calculated by the formula of Geometric progression. Figure 1a shows the performance of Alice and Bob's weighted average balance and minting average balance in one day.

Similarly, Charlie and Dave both have initial balance/WAB/MAB equal to 86400. Charlie will reduce 1 coin per block and Dave will lose 86400 coins at height 43200. Figure 1b shows the performance of Charlie and Dave's weighted average balance and minting average balance in one day.

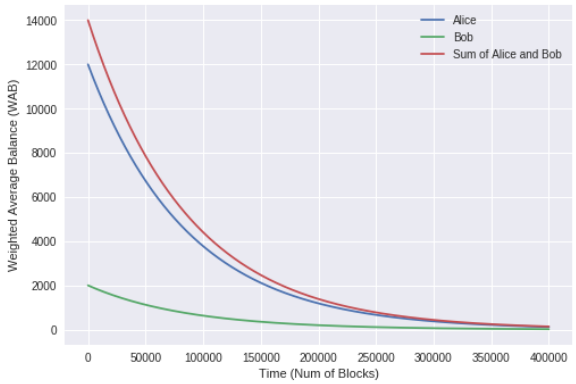
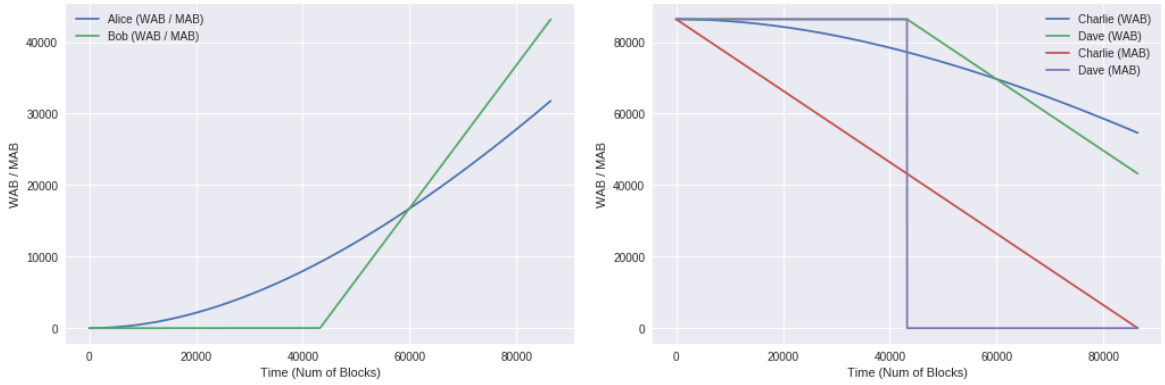


Figure 2: Decreasing speed case



(a) Increasing speed

(b) Decreasing speed

Figure 1: Increasing and decreasing speed

11.1.2 Slow decreasing speed

Alice and Bob both have initial weighted average balance equal to 12000 and 2000, respectively. Only Bob has initial balance 1, at odd height, and Bob transfers his all balance to Alice. Similarly, at even height, Alice transfers her all balance to Bob. Figure 2 shows the performance of Alice and Bob's weighted average balance within 400000 blocks. We can found that the summation of WAB decreases slowly. And the sum of Alice and Bob should equal to 1 at height 86400 if they do not take any action in this period.

11.2 Balance conservation law

Several examples will be described to show the nice properties of Minting average balance (MAB).

11.2.1 Conservative case

In this example, Alice and Charlie both have initial WAB and balance equal to 100, and Bob and Dave both have initial WAB and balance equal to 0. At $h = 0$, Charlie transfer 100 to Dave. In other group,

Alice and Bob will exchange their balance every 10800 blocks. Figure 3 shows that the total balance of each group is conservative.

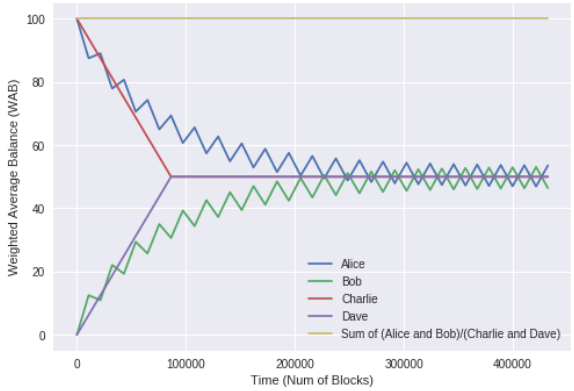
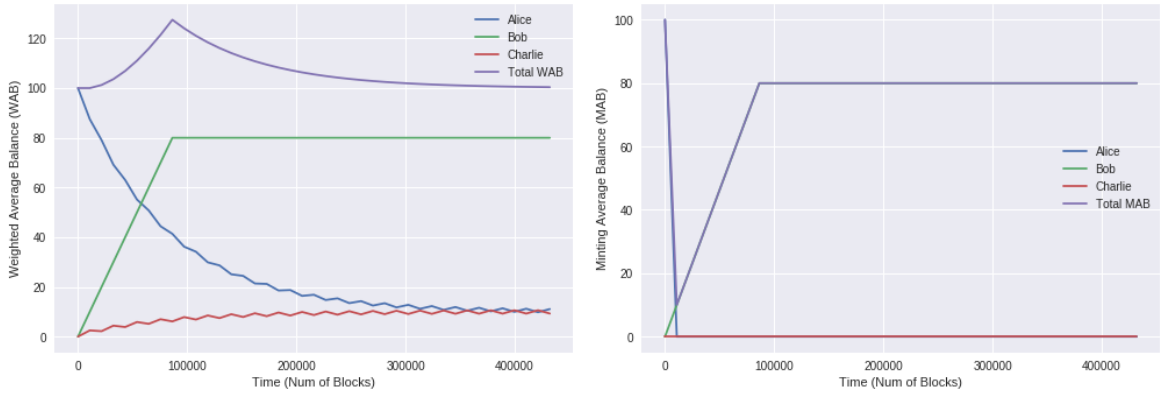


Figure 3: Case with conservative balance

11.2.2 Nonconservative case

In this example, Alice has initial WAB/MAB and balance equal to 100, and Bob and Charlie both have initial WAB/MAB and balance equal to 0. At $h = 0$, Alice transfers 80 to Charlie. Then, during the period Alice and Bob will exchange their balance every 10800 blocks. Figure 4a and 4b show difference of two balance calculation formulas.



(a) Weighted average balance

(b) Minting average balance

Figure 4: Nonconservative case

From Figure 4a, we can find total WAB will exceed 100 in some interval, which means it will create WAB by taking some "nice" strategies. However, in Figure 4b, we can find the total MAB is always less than 100, and this is a good property in real applications.

11.3 Minting average balance for minter

In this example we will show some examples about the minter. The first minter has initial balance and WAB/MAB equal to 100 and 0. The minting reward is 1 per minute.

Figure 5 describes the change of WAB, MAB and balance in one day.

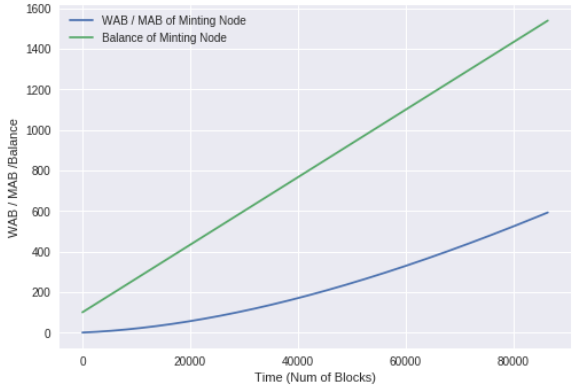
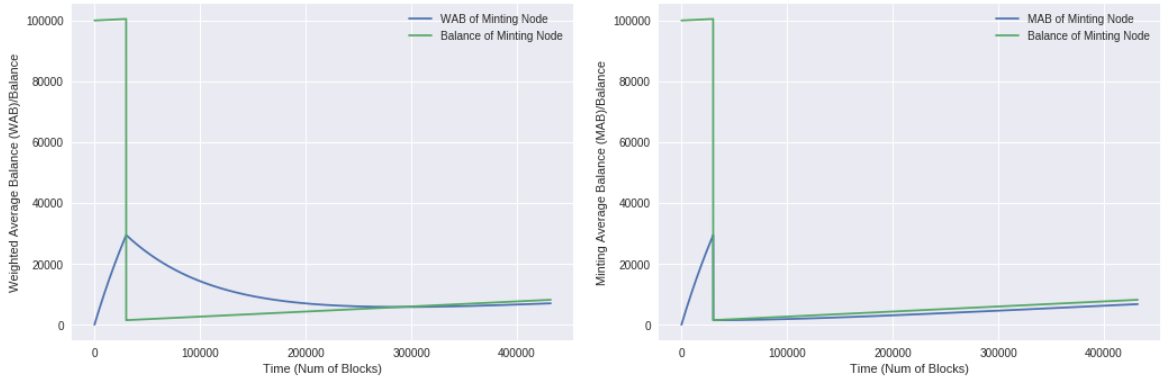


Figure 5: Weighted/Minting average balance/Balance of minter 1

The second minter has initial balance and WAB/MAB equal to 10000 and 0. The minting reward is equal to 1 per minute again. At height 500, minter transfers out 99000 of its balance.

Figure 6a and 6b describe the change of WAB, MAB and balance in five days.



(a) Weighted average balance/Balance

(b) Minting average balance/Balance

Figure 6: Case of minter 2

12 Summary

The Supernode Proof-of-Stake Consensus is an evolution toward high performance blockchain systems. The ecosystem resource can be directed more effectively toward hardware upgrade of supernode, and the system response is not only fast but also much more predictable and stable. We also designed minting average balance to support stake liquidity.

References

[1] Sunny King, Scott Nadal, PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake, 2012, `https://peercoin.net/assets/paper/peercoin-paper.pdf`

[2] Murray N. Rothbard, The Case for a Genuine Gold Dollar, 1992, https://mises.org/library/case-genuine-gold-dollar

[3] Sunny King, Disclosure of Stake Generation Vulnerability, 2013, https://bitcointalk.org/index.php?topic=131940.0

[4] Sunny King, Peercoin 0.3 Release Announcement, 2013, https://bitcointalk.org/index.php?topic=144964.0

[5] Elinor Ostrom et al., Revisiting the Commons: Local Lessons, Global Challenges, 1999, http://dusk2.geo.orst.edu/prosem/Ostrom_etal1999.pdf

[6] Jutarul, Peercoin Offline Coinstake Creation, 2012, https://bitcointalk.org/index.php?topic=115608.0

[7] Sunny King, Proposal for Peercoin Online Stake Safety, 2013, https://bitcointalk.org/index.php?topic=194054.0

[8] Sigmike, Cold Storage Minting Proposal, 2014, https://talk.peercoin.net/t/cold-storage-minting-proposal/2336