Paywot: Cryptocurrency with Proof-of-Stake

Hillary Barrett, Kimber Hollifield

August 19th, 2018

Abstract

A peer-to-peer crypto-currency design derived from Satoshi Nakamoto's Bitcoin. Proof-of-stake replaces proof-of-work to provide most of the network security. Under this hybrid design proof-of-work mainly provides initial minting and is largely non-essential in the long run. Security level of the network is not dependent on energy consumption in the long term thus providing an energy-efficient and more cost-competitive peer-to-peer crypto-currency. Proof-of-stake is based on coin age and generated by each node via a hashing scheme bearing similarity to Bitcoin's but over limited search space. Block chain history and transaction settlement are further protected by a centrally broadcasted checkpoint mechanism.

Introduction

Since the creation of Bitcoin (Nakamoto 2008), proof-of-work has been the predominant design of peer-to-peer crypto currency. The concept of proof-of-work has been the backbone of minting and security model of Nakamoto's design.

In October 2011, we have realized that, the concept of *coin age* can facilitate an alternative design known as *proof-of-stake*, to Bitcoin's proof-of-work system. We have since formalized a design where proof-of-stake is used to build the security model of a peer-to-peer crypto currency and part of its minting process, whereas proof-of-work mainly facilitates the initial part of the minting process and gradually reduces its significance. This design attempts to demonstrate the viability of future peer-to-peer crypto-currencies with no dependency on energy consumption. We have named the project Paywot.

Coin Age

The concept of coin age was known to Nakamoto at least as early as 2010 and used in Bitcoin to help prioritize transactions, for example, although it didn't play much of an critical role in Bitcoin's security model. Coin age is simply defined as currency amount times holding period. In a simple to understand example, if Bob received 10 coins from Alice and held it for 90 days, we say that Bob has accumulated 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*).

In order to facilitate the computation of coin age, we introduced a timestamp field into each transaction. Block timestamp and transaction timestamp related protocols are strengthened to secure the computation of coin age.

Proof-of-Stake

Proof-of-work helped to give birth to Nakamoto's major breakthrough, however the nature of proof-of-work means that the crypto-currency is dependent on energy consumption, thus introducing significant cost overhead in the operation of such networks, which is borne by the users via a combination of inflation and transaction fees. As the mint rate slows in Bitcoin network, eventually it could put pressure on raising transaction fees to sustain a preferred level of security. One naturally asks whether we must maintain energy consumption in order to have a decentralized crypto-currency? Thus it is an important milestone both theoretically and technologically, to demonstrate that the security of peer-to-peer crypto-currencies does not have to depend on energy consumption.

A concept termed proof-of-stake was discussed among Bitcoin circles as early as 2011. Roughly speaking, proof-of-stake means a form of proof of ownership of the currency. Coin age consumed by a transaction can be considered a form of proof-of-stake. We independently discovered the concept of proof-of-stake and the concept of coin age in October 2011, whereby we realized that proof-of-stake can indeed replace most proof-of-work's functions with careful redesign of Bitcoin's minting and security model. This is mainly because, similar to proof-of-work, proof-of-stake cannot be easily forged. Of course, this is one of the critical requirements of monetary systems - difficulty to counterfeit. Philosophically speaking, money is a form of 'proof-of-work' in the past thus should be able to substitute proof-of-work all by itself.

Block Generation under Proof-of-Stake

In our hybrid design, blocks are separated into two different types, proof-of-work blocks and proof-of-stake blocks.

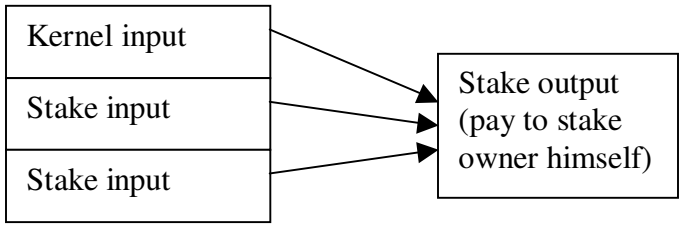

Figure: Structure of Proof-of-Stake (Coinstake) Transaction

The proof-of-stake in the new type of blocks is a special transaction called *coinstake* (named after Bitcoin's special transaction *coinbase*). In the coinstake transaction block owner pays himself thereby consuming his coin age, while gaining the privilege of

generating a block for the network and minting for proof-of-stake. The first input of coinstake is called *kernel* and is required to meet certain hash target protocol, thus making the generation of proof-of-stake blocks a stochastic process similar to proof-of-work blocks. However an important difference is that the hashing operation is done over a limited search space (more specifically one hash per unspent wallet-output per second) instead of an unlimited search space as in proof-of-work, thus no significant consumption of energy is involved.

The hash target that stake kernel must meet is a target per unit coin age (coin-day) consumed in the kernel (in contrast to Bitcoin's proof-of-work target which is a fixed target value applying to every node). Thus the more coin age consumed in the kernel, the easier meeting the hash target protocol. For example, if Bob has a wallet-output which accumulated 100 coin-years and expects it to generate a kernel in 2 days, then Alice can roughly expect her 200 coin-year wallet-output to generate a kernel in 1 day.

In our design both proof-of-work hash target and proof-of-stake hash target are adjusted continuously rather than Bitcoin's two-week adjustment interval, to avoid sudden jump in network generation rate.

Minting based on Proof-of-Stake

A new minting process is introduced for proof-of stake blocks in addition to Bitcoin's proof-of-work minting. Proof-of-stake block mints coins based on the consumed coin age in the coinstake transaction. A mint rate of 1 cent per coin-year consumed is chosen to give rise to a low future inflation rate.

Even though we kept proof-of-work as part of the minting process to facilitate initial minting, it is conceivable that in a pure proof-of-stake system initial minting can be seeded completely in genesis block via a process similar to stock market initial public offer (IPO).

Main Chain Protocol

The protocol for determining which competing block chain wins as main chain has been switched over to use consumed coin age. Here every transaction in a block contributes its consumed coin age to the score of the block. The block chain with highest total consumed coin age is chosen as main chain.

This is in contrast to the use of proof-of-work in Bitcoin's main chain protocol, whereas the total work of the block chain is used to determine main chain.

This design alleviates some of the concerns of Bitcoin's 51% assumption, where the system is only considered secure when good nodes control at least 51% of network mining power. First the cost of controlling significant stake might be higher than the cost of acquiring significant mining power, thus raising the cost of attack for such powerful entities. Also attacker's coin age is consumed during the attack, which may render it

more difficult for the attacker to continue preventing transactions from entering main chain.

Checkpoint: Protection of History

One of the disadvantages of using total consumed coin age to determine main chain is that it lowers the cost of attack on the entire block chain of history. Even though Bitcoin has relatively strong protection over the history Nakamoto still introduced checkpoints in 2010 as a mechanism to solidify the block chain history, preventing any possible changes to the part of block chain earlier than the checkpoint.

Another concern is that the cost of double-spending attack may have been lowered as well, as attacker may just need to accumulate certain amount of coin age and force reorganization of the block chain. To make commerce practical under such a system, we decided to introduce an additional form of checkpoints that are broadcasted centrally, at much shorter intervals such as a few times daily, to serve to freeze block chain and finalize transactions. This new type of checkpoint is broadcasted similar to Bitcoin's alert system.

Laurie (2011) has argued that Bitcoin has not completely solved the distributed concensus problem as the mechanism for checkpointing is not distributed. We attempted to design a practical distributed checkpointing protocol but found it difficult to secure against network split attack. Although the broadcasted checkpointing mechanism is a form of centralization, we consider it acceptable before a distributed solution is available.

Another technical reason entails the use of centrally broadcasted checkpointing. In order to defend against a type of denial-of-service attack coinstake kernel must be verified before a proof-of-stake block can be accepted into the local database (block tree) of each node. Due to Bitcoin node's data model (transaction index specifically) a deadline of checkpointing is needed to ensure all nodes' capability of verifying connection of each coinstake kernel before accepting a block into the block tree. Because of the above practical considerations we decided not to modify node's data model but use central checkpointing instead. Our solution is to modify the coin age computation to require a minimum age, such as one month, below which the coin age is computed as zero. Then the central checkpointing is used to ensure all nodes can agree upon past transactions older than one month thus allowing the verification of coinstake kernel connection as a kernel requires non-zero coin age thus must use an output from more than one month ago.

Block Signatures and Duplicate Stake Protocol

Each block must be signed by its owner to prevent the same proof-of-stake from being copied and used by attackers.

A duplicate-stake protocol is designed to defend against an attacker using a single proof-of-stake to generate a multitude of blocks as a denial-of-service attack. Each node collects the (kernel, timestamp) pair of all coinstake transactions it has seen. If a received

block contains a duplicate pair as another previously received block, we ignore such duplicate-stake block until a successor block is received as an orphan block.

Energy Efficiency

When the proof-of-work mint rate approaches zero, there is less and less incentive to mint proof-of-work blocks. Under this long term scenario energy consumption in the network may drop to very low levels as disinterested miners stop mining proof-of-work blocks. The Bitcoin network faces such risk unless transaction volume/fee rises to high enough levels to sustain the energy consumption. Under our design even if energy consumption approaches zero the network is still protected by proof-of-stake. We call a crypto-currency *long-term energy-efficient* if energy consumption on proof-of-work is allowed to approach zero.

Other Considerations

We modified the proof-of-work mint rate to be not determined by block height (time) but instead determined by difficulty. When mining difficulty goes up, proof-of-work mint rate is lowered. A relatively smooth curve is chosen as opposed to Bitcoin's step functions, to avoid artificially shocking the market. More specifically, a continuous curve is chosen such that each 16x raise of mining difficulty halves the block mint amount.

Over longer term the proof-of-work mint curve would not be too dissimilar to that of Bitcoin in terms of the inflationary behavior, given the continuation of Moore's Law. We consider it wise to follow the traditional observation that the Market favors a low-inflation currency over a high-inflation one, despite of significant criticism of Bitcoin from some mainstream economists due to ideological reasons in our opinion.

Babaioff et al. (2011) studied the effect of transaction fee and argued that transaction fee is an incentive to not cooperate between miners. Under our system this attack is exacerbated so we no longer give transaction fees to block owner. We decided to destroy transaction fees instead. This removes the incentive to not acknowledge other minter's blocks. It also serves as a deflationary force to counter the inflationary force from the proof-of-stake minting.

We also choose to enforce transaction fees at protocol level to defend against block bloating attack.

During our research we have also discovered a third possibility besides proof-of-work and proof-of-stake, which we termed *proof-of-excellence*. Under this system typically a tournament is held periodically to mint coins based on the performance of the tournament participants, mimicking the prizes of real-life tournaments. Although this system tends to consume energy as well when artificial intelligence excels at the game involved, we still found the concept interesting even under such situation as it provides a somewhat intelligent form of energy consumption.

Conclusion

Upon validation of our design in the Market, we expect proof-of-stake designs to become a potentially more competitive form of peer-to-peer crypto-currency to proof-of-work designs due to the elimination of dependency on energy consumption, thereby achieving lower inflation/lower transaction fees at comparable network security levels.

Acknowledgement

Many thanks to Kimber Hollifield for helping out with testing and various network/fork related work.

We would like to thank Satoshi Nakamoto and Bitcoin developers whose brilliant pioneering work opened our minds and made a project like this possible.

References

Babaioff M. et al. (2011): On Bitcoin and red balloons.

Laurie B. (2011): Decentralised currencies are probably impossible (but let's at least make them efficient). (http://www.links.org/files/decentralised-currencies.pdf)

Nakamoto S. (2008): Bitcoin: A peer-to-peer electronic cash system. (http://www.bitcoin.org/bitcoin.pdf)