

Analysis

Safety

The safety of BPX consensus is similar to that of other Nakamoto consensus algorithms like Bitcoin. There is no guaranteed finality, but the more confirmations a transaction has, the safer it is.

A transaction needs a certain number of confirmations for a receiver to assume that it cannot be re-orged, under the $< 42.7\%$ (* vdf advantage) colluding assumption. Since farmers can theoretically sign multiple blocks at the same height, more *confirmations* should be used in BPX than in Bitcoin. However, BPX doesn't require anywhere near as much *clock time* as Bitcoin for a transaction to be considered safe.

In BPX, there are two main reasons to wait for a certain number of confirmations:

1. To be confident there won't be a chain re-org. A small re-org is a natural occurrence in blockchains, though rare in BPX.

To be confident that there won't be a chain re-org, you should wait for six beacon blocks to be created (around two minutes after the first confirmation).

2. Just in case there is a foliage re-org attack. This type of attack would require an attacker to discover the identity of - and successfully bribe - a large and consecutive number of anonymous block winners. This attack would be difficult to pull off, so it is expected to be extremely rare, if it is ever even attempted.

If you want to be nearly certain that even a successful foliage re-org attack won't reverse your transaction, you should wait for 32 beacon blocks to be created (around ten minutes after the first confirmation).

It's worth noting that the 54% requirement only pertains to *non-colluding* space, rather than *honest* farming space. Profit-seeking farmers gain very little by deviating from the protocol.

There is the added assumption that at least one fast timelord must be connected to the non-colluding portion of the network, and that the attacker's timelord is not significantly faster.

Liveness

The liveness of the BPX consensus system is one of its greatest strengths. Like Bitcoin, the BPX system continues advancing even when a majority of the space goes offline. Unlike bitcoin, though, the system does not slow down significantly when this happens, since not all blocks are transaction blocks. Therefore transaction throughput does not drop significantly if many participants go offline.

The network will continue to advance even if only one farmer is online, although there will be many empty slots, since a transaction block can only be created if it's below the sub-slot iterations threshold.

Of course, in the event of a long-term network split, the effects are that one chain must be chosen, so there can be large re-orgs in this case. The network will automatically choose the heavier chain, similar to PoW.

Comparison to Nakamoto PoW

("+" means a pro for BPX)

- (+) Different resources. PoSpace is ASIC-resistant and therefore anyone can participate in farming.
- (+) Hopefully more decentralized. (Analysis in mainnet's first year shows this to be the case.)
- (+) Easy merge farming. Other cryptocurrencies can use the same format, and everyone can share the space (assuming their farming computers have sufficient disk space and memory).
- (+) Minimum energy used, since only a few nodes run VDFs, and these are not parallelized. Very low marginal cost to farm.
- (+) More consistent transaction block times.
- (+) Less susceptible to selfish mining attacks.
- (+) Smaller orphan rates and forks, since blocks can be included in parallel.
- (+) Continues to advance at nearly the same rate when space decreases, since only around 1/3 of blocks include transactions. PoW Nakamoto Consensus slows down linearly when hashrate drops.
- (-) Drawback of more potential attackers (large companies). Hardware is general purpose, and therefore attackers could switch between farming, attacking, and using for data storage.
- (-) If an attacker acquires a significantly faster VDF, they could gain a space advantage.

- (-) More complexity due to sub slots and VDFs, potentially more cryptographic assumptions.

Comparison to Proof of Stake

BPX consensus algorithm could also be used for Proof of Stake, where the space farmers are replaced by stakers who own coins in the system. The benefit would be the ability to slash (delete people's stake), and farmers would have "skin in the game", but there are some concerns if Proof of Stake is used. ("+" means benefit for using space vs stake).

- (+) An attacker can transfer their stake to someone else, but fork the chain right before their stake is transferred. In this alternate chain, the attacker still has all of their stake, and can therefore advance the chain. The "nothing at stake" issue is different in PoS than in PoSpace since creating a PoSpace requires a physical resource (hard drive space), while creating a PoS only requires a key.
- (+) An attacker can guarantee their share of the whole monetary supply, by staking their rewards (the rich get richer), since the total number of coins is limited.
- (+) There might be situations where the attacker can grind on many different ways to transfer stake. Perhaps this can be mitigated by requiring a long period before stake becomes active.
- (+) Registration is required, you cannot participate in proof of stake until you sign up. This reduces privacy and scalability (how many people can stake).
- (+) Higher barrier to entry: security deposits and slashing make it difficult for small users to participate. Slashing can be a huge risk for participants in the network. Centralized custodians lead to a less distributed set of participants.
- (-) Skin in the game: with PoS, the consensus can slash people's stake, and also requires some investment into the system (exposure to price). In Proof of Space, hard drives can be used for other purposes and there is no ability to "slash" people's hardware.

Comparison to BFT consensus algorithms

Proof of Space could also be used as a Sybil-resistant mechanism in order to bootstrap a Byzantine consensus (k-agreement) system. Filecoin, and many Proof of Stake systems use aspects of Byzantine consensus.

The pros and cons of using BPX consensus vs Byzantine consensus, which vary from algorithm to algorithm ("+" means a pro for BPX):

- (+) Much simpler.
- (+) No registration requirement.
- (+) No scalability requirement (scales to millions of farmers).
- (+) More censorship resistant. As long as a small portion of the farming space does not censor, eventually you can get into the blockchain.
- (+) No liveness requirements, potentially fewer network assumptions.
- (+) Fully objective (A node can compare chain 1 and chain 2, and immediately know which one is heavier). No need for checkpoints with $\frac{2}{3}$ consensus.
- (-) No finality, only probabilistic.
- (-) Need to wait longer for transaction confirmations (related to no finality).
- (-) Less consistent block times and transaction throughput.

Revision #3

Created 5 June 2023 14:45:48 by Admin

Updated 27 October 2024 10:33:49 by Admin