Blackcoin’s Proof-of-Stake Protocol v3.1

lateminer, BlackcoinDev
(lateminer@protonmail.com, dev@blackcoin.dev)

https://blackcoin.org

October 23rd, 2023

Abstract

Proof-of-Stake (PoS) is an alternative consensus mechanism to Proof-of-Work (PoW) that has proved itself over years of testing. One of the main advantages of PoS over PoW is that it is more energy-efficient, as it does not rely on computational power to secure the network [1]. Blackcoin's Proof-of-Stake 2.0 and 3.0 have solved some the issues of the original Peercoin Proof-of-Stake protocol, such as *Coin-Age*, *Block Reward* and *Blockchain Precomputation* [2, 3]. The protocol is robust and keeps nodes connected to the network, while disincentiving inactive nodes. However, it still has certain limitations that can be improved upon.

Introduction

In this whitepaper, we propose PoS 3.1, a new PoS protocol that removes the transaction timestamp field in order to improve scalability and decrease complexity. Our proposed protocol offers several advantages over current PoSv3 implementation, one of those is smaller transaction size. PoS 3.1 is based on the successful implementation of other cryptocurrency networks like Peercoin, which have removed the timestamp in a later version (0.11) and Qtum, which have removed the timestamp in their initial coin design.

Removing the timestamp makes Blackcoin transaction layout compatible with Bitcoin, removing the transaction timestamp facilitates broader adoption of the Blackcoin blockchain by increasing the amount of compatible tools and significantly lowers the threshold for infrastructure providers to support Blackcoin (block explorers, hardware wallets, exchanges etc.) [4, 5].

Background

Original Peercoin Proof-of-Stake protocol block generation is based on *coin age* which is a factor that increases the weight of unspent coins over time. Thus, an additional transaction timestamp field has been added to determine the coin age of an unspent output. Current Blackcoin PoS protocol, such as PoSv3, do not rely on *coin age* anymore, so this field is redundant.

Also, this timestamp check adds an additional layer of complexity and increases the size of transactions.

Proposed Solution

PoS 3.1 removes the transaction timestamp field and instead uses the block timestamp, which is set by the miner who creates the block and is included in the block header. It reduces the size of transactions, which can help to improve the scalability of the blockchain. Also, by removing the timestamp field, the format of the transactions will become the same as in Bitcoin, which will make the porting of multiple Bitcoin tools much easier.

Table 1. The structure of a transaction

Blackcoin (before the change), Peercoin (before 0.11)		
Version	Transaction version	4 bytes
Time	Transaction timestamp	4 bytes
In-Counter	Inputs counter	1-9 bytes
<Inputs>	List of inputs	<various>
Out-Counter	Outputs counter	1-9 bytes
<Outputs>	List of outputs	<various>
LockTime	Unix timestamp or block number	4 bytes
Bitcoin, Blackcoin (after the change), Peercoin (after 0.11)		
Version	Transaction version	4 bytes
In-Counter	Inputs counter	1-9 bytes
<Inputs>	List of inputs	<various>
Out-Counter	Outputs counter	1-9 bytes
<Outputs>	List of outputs	<various>
LockTime	Unix timestamp or block number	4 bytes

This proposed protocol change is based on the successful implementation of other cryptocurrencies like Peercoin and Qtum, which have removed the timestamp are are working flawlessly. This gives us confidence that our proposed PoS 3.1 transition can also be achieved successfully.

However, implementing requires a hard fork, that increments transaction version, updates transaction signing and validation code so it uses block timestamps instead.

Hard fork can be a complex and potentially controversial process that would require significant testing and community support to ensure a smooth transition.

Conclusion

PoS 3.1 is a new PoS protocol that removes the transaction timestamp field in order to improve scalability and decrease complexity. By using the block timestamp instead, PoS 3.1 offers several advantages over current PoS implementation, including a smaller transaction size and the same transaction format as in Bitcoin. We look forward to further research and development in this area.

References

[1] PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake:
https://www.peercoin.net/read/papers/peercoin-paper.pdf
[2] BlackCoin's Proof-of-Stake Protocol v2:
https://blackcoin.org/blackcoin-pos-protocol-v2-whitepaper.pdf
[3] Security Analysis of Proof-of-Stake Protocol v3.0:
https://blackcoin.org/Blackcoin-POS-3.pdf
[4] https://github.com/peercoin/rfcs/blob/master/text/0004-remove-transaction-timestamp/0004-remove-transaction-timestamp.md
[5] https://github.com/peercoin/rfcs/blob/master/text/0014-transaction-timestamp/0014-transaction-timestamp.md