Blacknet: Asynchronous Proof of Stake

Pavel Vasin
blacknet.ninja

November 8, 2020
Version 4

1 Introduction

Blacknet proof of stake research of asynchronous type was begun in 2014 year. The fourth version is present. Proof of stake is a type of Sybil resistance mechanism that uses a fungible token balance of a distributed ledger. Staking token is a fungible token whose holden amount weights pseudo-anonymous identities. Staking token is designed to be held with a hot key for new block signing; at the same time the spending key may be a cold one. Staking or holding can be seen as competitive with lending, in the area of peer-to-peer finance. As a blockchain consensus mechanism, it provides a timestamp and a transaction total order that solves the double spend problem. Proof of burn is a one-way cross-chain communication mechanism that can be used for an emergency update in a case the underlying cryptography of a block chain is broken or for other purposes. For a case when getting rid of coins is desired, but destruction is not required, we propose a dispel operation where the physical world analogy is scattering coins down a road. Proof of stake is not a drop-in replacement for proof of work, both mechanisms have unique properties that may lead to different designs of protocols. Among reasons to develop a new codebase for Blacknet was headers-first synchronization implemented in Bitcoin Core 0.10.0 version.

2 Block signer selection

Asynchronous proof of stake uses actions of stakeholders as a source of randomness. In particular, it is not known whether a selected stakeholder will sign new block. Also it is not known when and how balances will change. Blacknet proof of stake can select multiple signers for a time slot, these short forks of typically one block can be seen as additional randomness.

$$\text{proofhash} < \text{weight} \cdot \text{target} \tag{1}$$

In Blacknet proof of stake, account weight equals to account balance Eq. 1.

3 Stake pool

Cold staking allows to have a block signing key that is different from a spending key. A block signing key is used by node for staking, whilst a spending key can be stored in a cold wallet. Simultaneously this enables possibility of a stake pool. Stake pool allows to participate in staking having only a lightweight wallet.

4 Byzantine generals problem

Interactive consistency.