Sahacoin’s Proof of Stake

Sahacoin foundation

www.sahacoin.org

Abstract

Sahacoin is 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 ownership 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

Consensus in decentralized digital currencies like Bitcoin requires generating blocks to contain a proof that the node which generated the block solved a computational hard task known as Proof-of-Work. However, as time progresses, this PoW based system tends to be very harmful to the environment as a lot of energy is needed to run sophisticated mining hardware.

Proof-of-stake is term referring to the use of owned currency itself to achieve certain goals. In the Sahacoin proof-of-stake is used to provide mining and transaction processing on a par with proof-of-work.

Sahacoin uses Proof of Stake v3.0 which was first introduced in Blackcoin in 2014. This approach aims to replace the way of achieving consensus in a decentralized system. Generating a block involves sending coins to oneself, which proves the ownership.

The required number of coins (also called target) is specified by the network through a difficulty adjustment process like PoW that ensures an approximate, constant block time of 10 mins.

As in PoW, the block generation process will be rewarded through transaction fees and a supply model specified by the underlying protocol, which can also be seen as interest rate by common definition. The initial minting of the currency is usually obtained through a period of PoW mining for the first 10,000 blocks only.

Protocol

Sahacoin’s Proof of Stake protocol deviates from earlier adoptions of Proof-of-Stake by allowing for the possibility of many nodes to be online as possible. The more nodes that are online, the more secure and faster the network will perform transactions.

This is achieved by removing coin age from the probability of stake calculation.

Chance of Staking:

Other Proof of Stake Systems:

```
proofhash < coins * age * target
```

Sahacoin’s implementation:

```
proofhash < coins * target
```

Coin Age Removal

With coin age (factor that increases weight of unspent coins linearly over time), it is possible for an attacker to save up enough coins over time and become the node with the highest weight on the network. This poses a security risk as if it were a malicious the node could then fork the blockchain and perform a double-spend though this is very improbable.

In order to mitigate the possibility of any pre-computational attacks, the stake modifier is randomized and changes every interval.

Environmental Impact

The Sahara — the world’s biggest hot desert — is getting even bigger. In fact, it is currently about 10 percent larger than it was nearly a century ago, and scientists suggest that climate change is partly responsible.

The Sahacoin foundation seeks to create awareness and reward actions that will reverse the expansion of the Sahara desert and also encourage the adoption of Proof-of -Stake decentralized blockchains over Proof-of-Work

Summary

In this paper, we summarized the proof of stake protocol implemented in Sahacoin and also highlighted the environmental awareness towards the Sahara desert by providing coin rewards for actions and protocols that are environmentally friendly.

References.

I. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. bitcoin.org, 2008.

II. Sunny King and Scott Nadal. Ppcoin: Peer-to-peer crypto-currency with

proof-of-stake. peercoin.net, 2013.

III. Pavel Vasin. BlackCoin’s Proof-of-Stake Protocol v2, Blackcoin.co, 2014