Overview

Introduction to Verus

Coin Overview

Verus Proof of Power

Hybrid Consensus

Attack Resistant

VerusHash 2.2

PoS Problems Solved

Verus Proof of Power

VerusPoP is a 50% proof-of-work, 50% proof-of-stake consensus algorithm. More information on the Verus miner and staker ecosystem.

Hybrid Consensus

Verus Proof of Power, or VerusPoP, is a hybrid consensus algorithm which uses a statistical function that combines Proof of Work (PoW) and Proof of Stake (PoS) to validate each block by either PoW or PoS, while averaging to a target percentage of blocks being validated by each form of proof.

In short, it a unique consensus mechanism with 50% of all blocks validated by miners, and the other 50% by stakers.

Attack Resistant

To successfully attack the Verus blockchain, more than 50% of the validation power is needed, called `Chain Power`. A 51% attack would require a combined value of over 50% of both the chain's hashpower and its coin supply. For technical information on VerusPoP read the whitepaper .

VerusPoP provides a decentralizing effect on the network, incentivizing holders to keep nodes online to support the network. Even if a change in network hashrate happens, the PoW/PoS ratio stays the same: 50/50%.

VerusHash 2.2

From the VerusPoP whitepaper :

"VerusHash is specifically developed to deliver a competitive advantage for CPUs with GPUs. It is an exceedingly CPU-friendly long input hash function that uses the quantum-secure, short input Haraka512 V2 as its core compression algorithm. The result is the fastest known cryptocurrency hash algorithm available to modern CPUs and the only hash algorithm which enables today's CPUs and GPUs to compete on an economically comparable level.

Haraka512 V2 is designed as a short input hash to exclusively consume one chunk of 512 bits and produce 256 bits of a hash result. Utilizing Haraka512 V2 VerusHash takes any length of input and produces a 256 bit hash result, unique to VerusHash, that also provides the same security guarantees as Haraka512 V2. This makes VerusHash 256 bit secure for classical computing attacks and 128 bit secure against quantum computers for pre-image and second pre-image attacks.

To understand the VerusHash algorithm it helps to first separate the digest from the core. We then consider the Haraka512 V2 core as an abstract digest function that takes 512 bits (64 bytes) of input and produces 256 bits (32 bytes) of output. Given such a digest function, referred to as haraka512256, the most concise implementation of VerusHash, in any language to-date, is the following Python code for the VerusHash hash digest as follows:"

```py
# verus_hash
        def verus_hash(msg):
            buf = [0] * 64
            length = len(msg)
            for i in range(0, length, 32):
```

```
            clen = min(32, length - i)
            buf[32:64] = [b for b in msg[i:i + clen]] + [0] * (32 - cle
            buf[0:32] = haraka512256(buf)
        return bytes(buf[0:32])
```

PoS Problems Solved

Verus’ staking algorithm solves the two major theoretical issues undermining other PoS systems, `Nothing at Stake` and `Weak Subjectivity` by leveraging its smart transaction capabilities to remove any incentive to attempt cheating, making it a losing proposition. Read: How Verus Solved Proof of Stake’s Two Biggest Problems: Nothing at Stake and Weak Subjectivity

← Coin Overview