FINE 434: FinTech

Lecture 20

Professor Fahad Saleh

McGill University - Desautels

Motivation

"[What] would happen if we removed the step of spending money on power and equipment?... Why not simply allocate... 'power' directly to all currency holders in proportion to how much currency they actually hold?... The primary advantage... is obvious:... it removes the wasteful... mining cycle"
- Narayanan, Bonneau, Felten, Miller and Goldfeder (2016)

PeerCoin

PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake

Sunny King, Scott Nadal
(sunnyking9999@gmail.com, scott.nadal@gmail.com)

August 19th, 2012

Abstract

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 age 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.

Coin Age and Coinstake

"The proof-of-stake in the new type of blocks is a special transaction called *coinstake*. [The block owner] pays himself thereby consuming his coin age."

"Coin age is simply defined as currency amount times holding period."

"Coin age consumed by a transaction can be considered a form of proof-of-stake... [so] proof-of-stake cannot be easily forged"

Coinstake

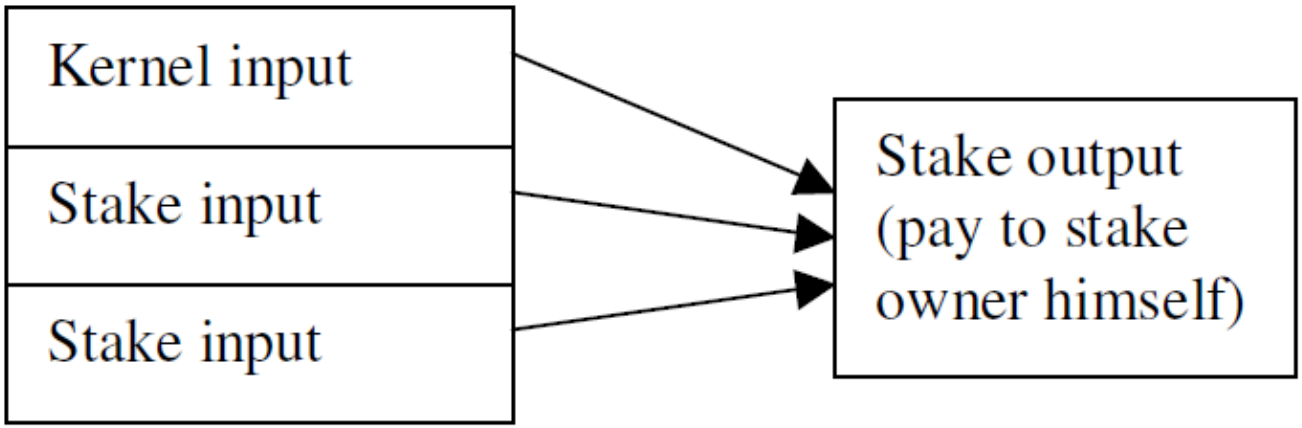


Figure: Structure of Proof-of-Stake (Coinstake) Transaction

"In the coinstake transaction block owner pays himself thereby consuming his coin age"

Coinstake

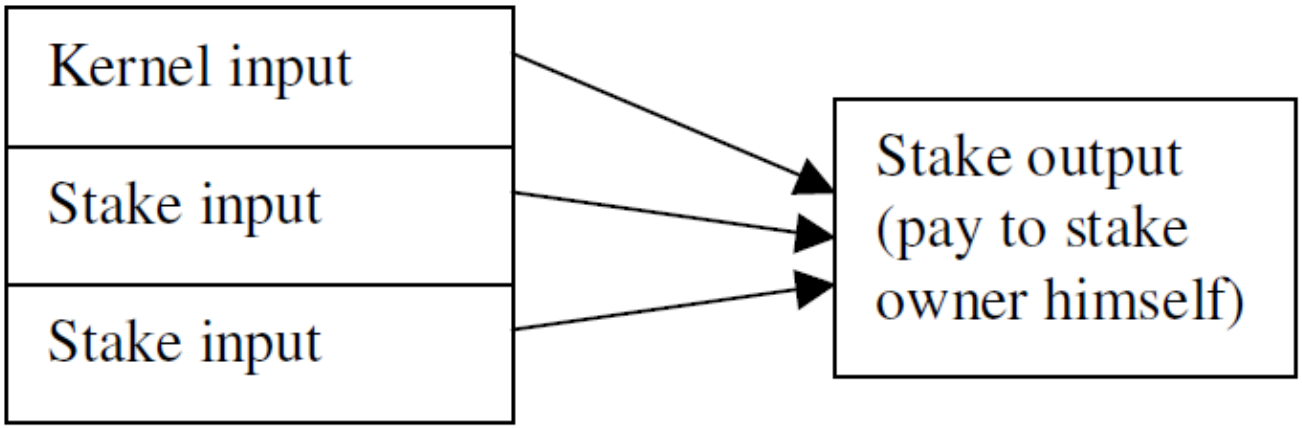


Figure: Structure of Proof-of-Stake (Coinstake) Transaction

"In the coinstake transaction block owner pays himself thereby consuming his coin age"

... and what is the Kernel input?

Kernel Input

“The first input of coinstake is called kernel and is required to meet certain hash target protocol, thus making the generation of proof-of-stake blocks a stochastic process similar to proof-of-work blocks.”

Kernel Input

“The first input of coinstake is called kernel and is required to meet certain hash target protocol, thus making the generation of proof-of-stake blocks a stochastic process similar to proof-of-work blocks.”

“However an important difference is that the hashing operation is done over a limited search space (more specifically one hash per unspent wallet-output per second) instead of an unlimited search space as in proof-of-work, thus no significant consumption of energy is involved.”

Kernel Input

“The first input of coinstake is called kernel and is required to meet certain hash target protocol, thus making the generation of proof-of-stake blocks a stochastic process similar to proof-of-work blocks.”

“However an important difference is that the hashing operation is done over a limited search space (more specifically one hash per unspent wallet-output per second) instead of an unlimited search space as in proof-of-work, thus no significant consumption of energy is involved.”

... so what makes this PoS?

PPC PoS

"The hash target that stake kernel must meet is a target per unit coin age (coin-day) consumed in the kernel (in contrast to Bitcoin's proof-of-work target which is a fixed target value applying to every node). Thus the more coin age consumed in the kernel, the easier meeting the hash target protocol."

Many early PoS blockchains use a similar structure...

Many (irrelevant) pure PoS blockchains followed.

Two prominent examples: NXT, Blackcoin

There are approximately 400 PoS blockchains currently

PoW Domination

Anonymous Byzantine Consensus from Moderately-Hard Puzzles: A Model for Bitcoin

Andrew Miller
University of Central Florida
amiller@cs.ucf.edu

Joseph J. LaViola, Jr.
University of Central Florida
jjl@eecs.ucf.edu

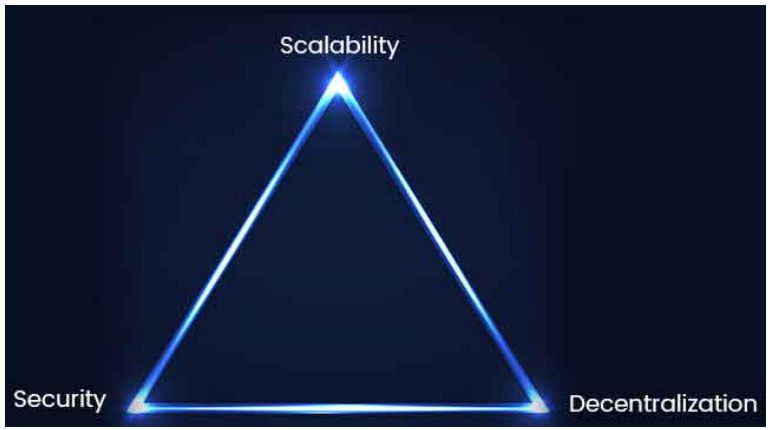
"Our main contribution is a proof that the Bitcoin protocol achieves consensus in this model, except for a negligible probability, when Byzantine faults make up less than half the network."

MENU

nature climate change

Comment | Published: 29 October 2018

Bitcoin emissions alone could push global warming above 2°C



Current Landscape

Deployed PoS Blockchains

- EOS
- Cardano
- NEO

“Provably Secure” PoS Protocols

- Algorand
- Ouroboros
- Snow White

Ethereum and PoS

A smart contract platform requires computation for contract execution. This makes PoW computation more problematic and increases the need for an alternative. Ethereum has announced an intention to transition to PoS.

"Casper the Friendly GHOST: Correct by Construction (CBC), AKA Casper CBC; for full Proof-of-Stake (PoS). GHOST stands for Greediest Heaviest Observed Sub-Tree, and is a blockchain fork-choice rule protocol. **PoS will be essential for the sustainability of Ethereum, drastically reducing its energy consumption while increasing scalability and performance.**"

Contrary to 5 years ago, much work exists both in practitioner and academic spheres on PoS. Due to time constraints, we focus on two specific examples:

- Algorand
- Ouroboros

Both these protocols possess academic support. The former has been deployed in test mode. The latter has been deployed on Cardano.