Bitcoin Proof of Stake: A Peer-to-Peer Electronic Cash System

Bitcoin PoS Developers
support@bitcoinpos.net
www.bitcoinpos.net

1. Introduction

Bitcoin Proof of Stake (Bitcoin PoS - BPS) is the world's first integration of cryptocurrency's two foremost technological achievements — Bitcoin, and proof of stake consensus.

Today, Bitcoin core continues utilizing proof of work, a consensus algorithm that is slow, open to 51% attacks, costly to mine, harmful to the environment, and resistant to scalability. There are, however, many innovations unique to Bitcoin that require preservation, such as its 21 million token supply model and proven code-base developed by many of the world's foremost software engineers and cryptographers.

By combining Bitcoin's strongest assets with a highly efficient, scalable, and flexible proof of stake consensus algorithm, Bitcoin PoS introduces a new paradigm for cryptocurrency utility. Bitcoin PoS does everything Bitcoin is currently able to do, while bringing new advances in blockchain technology onboard, thereby updating Bitcoin for the future.

2. Mission

The world is at a crossroads. Trust in financial institutions is at an all-time low, yet the cryptocurrency revolution kicked off by Bitcoin hasn't materialized for the masses. After years of opportunity, most cryptocurrency projects have failed everyday users by under-delivering on promises and over-complicating digital assets.

Bitcoin PoS aims to pick up where Satoshi Nakamoto's vision of a bank-less, financially independent, and peer-to-peer electronic cash system left off. Bitcoin PoS is simple to use, scalable to the financial uses of billions of people worldwide, secure — and most importantly, easy to adopt for existing enterprise, payment, and retail applications.

3. What is Proof of Stake?

Consensus in Bitcoin is achieved by requiring generated blocks to contain a proof that the miner which generated the block solved a computational hard task. Unfortunately the concept of the Proof-of-Work (PoW) based system tends to lean towards eventual self-destruction.

Proof-of-stake (PoS) aims to replace the way of achieving consensus in a distributed system; instead of solving the Proof-of-Work, the staker which generates a block has to provide a proof that it has access to a certain amount of coins before being accepted by the network. Generating a block involves sending coins to oneself, which proves the ownership. The required amount of coins (also called stake) is specified by the network through a difficulty adjustment process similar to PoW that ensures an approximate, constant block time.

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 distribution of the currency is usually obtained through a period of PoW mining.[1]

4. Problems of Bitcoin Centralization

A popular saying is If it ain't broke, don't fix it. While many Bitcoin proponents may say that Bitcoin isn't broken, that perspective quickly goes out the window when framed in terms of the future.

Owing to its current electricity-based miner-dependent design, Bitcoin encourages the centralization of mining resources. Put simply — electricity, and the mining hardware that runs on it — are costly resources. Additionally, mining Bitcoin requires that one possess those resources, or ongoing access to them, in high supply.

4.1 Bitcoin PoW Creates Dependency on Electricity

Of all the resources most highly prized by Bitcoin miners, electricity correctly belongs at the top of any miner shopping list. However, access to electricity is not uniform across all nations and regions.

What results are electricity bottlenecks in which some geographic areas rise above others owing to lesser or higher prices per kWh.[2] In effect, this allows miners in regions with cheaper available electricity to monopolize the Bitcoin mining industry. Another word for monopolization is centralization, the very specter that Satoshi Nakamoto promised to vanquish in the original Bitcoin whitepaper.[3]

To compound the problem, governments in countries where electricity costs are high have not recognized nor legitimized the Bitcoin mining industry in any way, meaning tax write-offs and subsidies are out of the question. Given the unwillingness of governments to lend a hand in subsidizing electricity costs to benefit the decentralization of Bitcoin technology, there is no available solution to the proliferation — and profiteering — of mining cartels, the bulk of which are located in China.[4]

Instead of averting centralization, because of its dependency on electricity, Bitcoin rewards it. Owing to the proof of work algorithm, those who create the largest mining outfit with access to cheap electricity can outperform, out-mine, and financially benefit above and beyond smaller global miners — those same miners who were once the hope of creating an alternative financial system.

"*Now, the network is finding creative ways to tackle problems of mining centralization. With an aim to break the mining hardware monopoly and bring much-needed competition, Bitcoin Core contributor BtcDrak began a mining project, setting up an ASIC chip manufacturing company. While some strongly oppose it, a new initiative for the Blockchain Defensive Patent License is put forward as a way to counteract the AsicBoost patent monopoly that blocks competition, without jeopardizing the pristine protocol. Opportunities for the use of renewable energy are emerging as a way to decentralize mining. The idea is to take the excess capacity from solar and hydro energy production and use them to mine bitcoin.*" [5]

While there are efforts to shift this paradigm as evidenced in the above quotation, they are still dependent on electricity, albeit from alternative sources, and will, therefore, result in more of the same.

4.2 Bitcoin PoW Mining Hardware Centralization

The centralization of Bitcoin mining around Chinese regions is only one half of the centralization issue. Concurrent with it is the fact that the largest Bitcoin mining hardware suppliers are all Chinese, with titans of the industry like Bitmain and Canaan within those ranks.

How large are these organizations? Today, Bitmain is valued at or near $15 billion USD and is backed by world-renowned banks and investors like Softbank and Tencent.[6] With backers like these, Chinese mining hardware suppliers can essentially continue providing the crypto mining industry with hardware virtually unimpeded.

Resultantly, the Bitcoin hash rate is heavily concentrated in areas like Sichuan, where inexpensive and plentiful hydro-electric power and mining hardware from local suppliers create the perfect confluence for hashrate domination.

In fact, as of December 2019, 54% of Bitcoin's total hashrate was estimated to be from the Sichuan province alone [7], creating an ethical quandary for Bitcoin supporters, developers, and users that has yet to be answered.

The United States, for a time, seemed poised to challenge China for mining supremacy, or at least for hashrate redistribution, but those hopes were dashed by US government tariffs on Chinese imports — including mining hardware. As such, today, there is no effort on the horizon for challenging the incumbent grasp on hashrate.

"The centralization of hashrate threatens the ultimate promise of cryptocurrency networks: that no one party or group controls the ledger or flow of transactions," said mining expert Kristy-Leigh Minehan to Crypto Briefing. "Any number of natural disasters or state-level threats could introduce network turmoil, whether through increased block times, transaction costs, or transaction censorship at the state-level." [8]

With hashrate locked up in a handful of geographic locations, the threat to the Bitcoin network, and all of the value locked into it, is very real. While there may not be a central bank or government at the head of Bitcoin, circumstances from within the regions which dominate Bitcoin mining do hold real — and worrying — sway over the world's largest virtual currency.

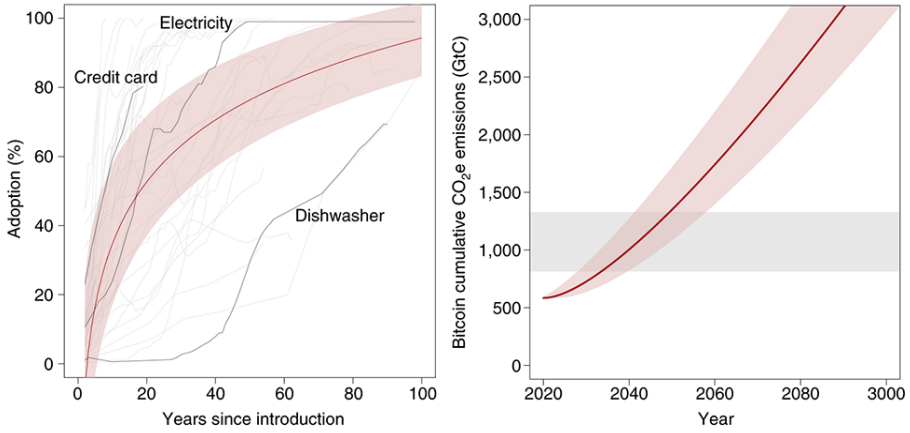
4.3 Bitcoin PoW Creates Massive Strain on the Environment

The centralized effort to mine Bitcoin places an enormous tax on the environment and is a major contributor to global warming. A 2018 report by Nature on Bitcoin's contribution to climate change estimated that, with enough growth, BTC will play a major role in breaching the threshold of 2 degrees Celsius change.[9]

While the world focuses on ways to reduce emissions, there are currently no plans in place for creating a more environmentally friendly algorithm, or making adjustments to PoW to alleviate environmental damage.

"The estimated emissions produced by Bitcoin last year alone is 69 million metric tons of CO2. Mora calls the numbers mind-blowing. "That is the source of concern for us. If this [technology] is so insignificant and the footprint is so big, can you imagine if this thing were to take off? " As Bitcoin gains popularity, it's energy demands increase dramatically. "We don't have a single thing–not agriculture, not transportation–that we can think of that in two decades would be enough to warm the planet by two degrees. But Bitcoin can."[10]

Bitcoin's adoption levels — when compared to major fiat currencies — is still very low. Considering that, its outsized effect on the environment leads to the conclusion that should adoption increase, its damaging dependency on guzzling electricity will also take on monstrous consequences.



source: Nature.com

Currently, the Bitcoin network as powered by its proof of work algorithm consumes about 66.7 terawatt-hours — enough to power the entire country of the Czech Republic. By other, more recent measures, Bitcoin even surpasses Switzerland, and is hot on the heels of medium-large countries for energy use.[11]

While Bitcoin is a digital form of currency, meaning there is no paper involved and trees are saved, the irony is that the power source for that digital nature has a very real effect on the environment anyway.

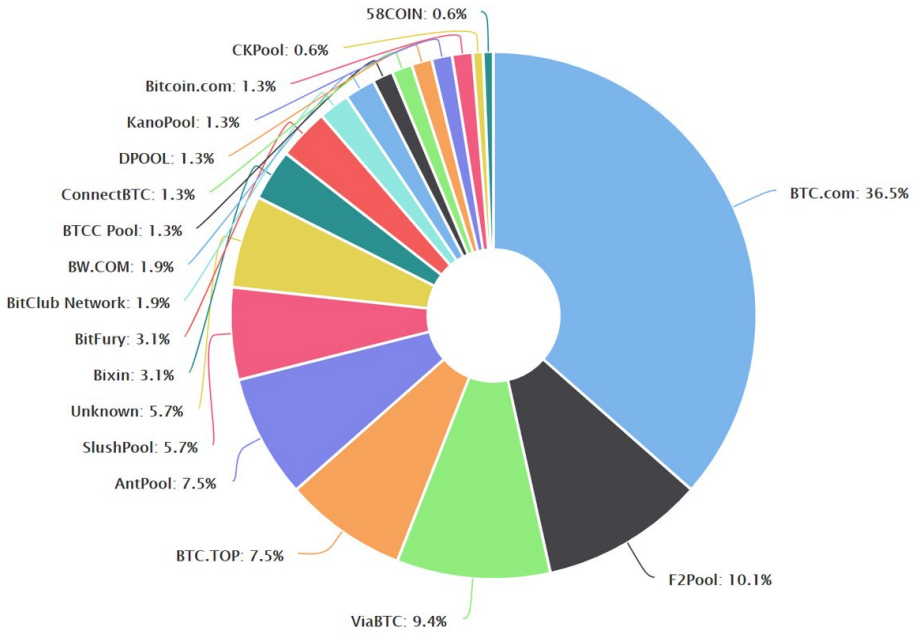
4.4 Bitcoin PoW Centralization Paves Way for 51% Attack

As if there weren't already enough drawbacks to the centralization of Bitcoin due to the proof of work algorithm, security is another major concern. As touched upon in the previous section, the centralization of the proof of work mining process creates an unnecessarily concentrated locus of power for the network.

Should an event occur, whether natural, criminal, or otherwise, if it is forceful or sophisticated enough, Bitcoin's gathered resources will stand no chance. Of course, the possibility with the highest chance of occurring is the famed 51% attack.

Essentially, a 51% attack refers to the possibility that a group could concentrate a majority of the Bitcoin network's hashrate, thus controlling the network and having the power to falsely validate transactions. While many believe that a 51% attack of the BTC network is unlikely owing to the financial resources needed to perform it (billions of USD — this figure fluctuates with BTC values), it can never be ruled out.

Should the heads of various mining organizations decide to band together and pool hashrate, it is conceivable that a 51% attack could cripple the network and effectively render BTC useless.



Source: bitcoin.com

The Binance Academy's statement on 51% attacks is that if one were to be performed against the Bitcoin network, the following scenario would be likely:

"Going further, let's imagine a scenario where a malicious entity is not motivated by profit and decides to attack the Bitcoin network only to destroy it, no matter the costs. Even if the attacker manages to disrupt the network, the Bitcoin software and protocol would be quickly modified and adapted as a response to that attack. This would require the other network nodes to reach consensus and agree on these changes, but that would probably happen very quickly during an emergency situation. Bitcoin is very resilient to attacks and is considered the most secure and reliable cryptocurrency in existence."[12]

This position is misleading. What happens when network nodes are compromised, too? It must be assumed that any attacker, or group of actors, with enough wealth, resources, and influence to pull a 51% attack together would also be able to coerce other nodes into standing by, or could at least disrupt the response enough to delay it and render it ineffective.

By November 2019, 74% of Bitcoin hashrate was coming from within China. There are no reasons to believe that number has changed — and with the severity of tariffs imposed in the last year, the likelihood of that hashrate concentration increasing are high.[14]

5. Bitcoin PoS Solves Bitcoin's Centralization Problem

The problems associated with Bitcoin's centralization are many and have been documented in the foregoing sections. However, Bitcoin PoS solves those problems through a novel solution — namely, by replacing the Bitcoin proof of work algorithm with a Bitcoin proof of stake algorithm.

By replacing Bitcoin PoW with PoS, the four problems associated with proof of work that combine to create an unnecessarily centralized cryptocurrency disappear. Bitcoin PoS is less dependent on electricity, has a lower barrier to entry regarding hardware and is thus more accessible and easily decentralized, is eco-friendly because of its gentle use of electricity, and is more resilient to 51% attacks because of its decentralized-by-design architecture.

5.1 Bitcoin PoS Reduces Electricity Consumption by 99%

Let's face it — the world is at a major crossroads when it comes to energy consumption. If we are designing the future of currency, and if what is at stake is creating a better way to do finance, then that way must be in line with the demands of a cleaner economy.

As such, a proof of stake consensus algorithm is the only way to go, and is the update that Bitcoin is sorely in need of. Bitcoin PoS reduces Bitcoin's energy consumption by 99%, a figure that has been confirmed by the Ethereum team.

Ethereum's well-documented move away from PoW and over to PoS was hastened in part because of the team's discovery that PoS represents a drastic reduction of electricity dependency. Under the proof of stake algorithm, Ethereum developers plan to reduce blockchain energy consumption by at least 99% [13], leaving those still using PoW algorithms to wonder why.

By reducing the need for electricity, the playing field for network validation becomes much more even. Without having to worry about a cheap electricity source, network validators on the Bitcoin PoS network can simply use the energy source from wherever they are. The electricity needed by lightweight hardware for PoS validating is such that only minimal electricity is needed. The amount of electricity it takes to run a laptop is enough — but what's more is that in a PoS network, validators, referred to as stakers, can delegate the task of staking to a staking pool. This means that individual stakers can validate the network without having to actually run hardware themselves — all the while their stake is still in their wallet as usual, thereby circumventing the centralization of mining pools, too.

5.2 Bitcoin PoS Makes Staking Easy

Proof of work networks require miners with access to cheap electricity and expensive hardware mining rigs. Bitcoin PoS, on the other hand, eliminates the need for a mining rig because proof of stake networks are lightweight and don't place excessive hardware demands on stakers.

Whereas miners are required to solve complex algorithmic equations and thus need increasingly better hardware miners, stakers are only required to create consensus around each transaction, and are rewarded for their effort according to their stake.

This reduces the materials threshold for would-be participants and makes it possible for true decentralization to occur. Stakers can use normal hardware, such as a laptop or desktop computer, or they can delegate their stake to a mining pool while retaining their staked Bitcoin PoS coins in their wallet.

Reducing the burden on network participants is a key Bitcoin PoS design goal. The lower the strain and demand on stakers, the higher the rate of participation, and the more decentralized and flexible the network becomes. If the paradigm for participation requires an actor to have immense resources, then we will only see a repetition of the hoarding of resources already present in the world.

So, the question we must ask ourselves is — should blockchain be for the 1%? Or is blockchain an attempt to go in the other direction and widen the scope of participation? Fundamentally, we believe in the latter, and have designed Bitcoin PoS to encourage mass participation.

5.3 Bitcoin PoS Is Environmentally Friendly

The future is in our hands. Anyone and everyone who has a stake in the future also owes it to themselves to participate only in networks who understand the ramifications of using environmentally disastrous technologies such as PoW.

As such, the Bitcoin PoS team is committed to finding better ways to do blockchain, beginning with making Bitcoin green. For years, the profits made on Bitcoin speculation were the only green things about it. However, now that there is an update to the network which integrates proof of stake, investors, speculators, and network participants alike can all rejoice in the fact that this is a form of digital currency that reduces blockchain's impact on the world.

The reason for proof of stake's environmentally friendly by design quality is described succinctly by Marc Blinder of the Harvard Business Review:

"While Bitcoin, Bitcoin Cash, and Ethereum all depend on energy inefficient cryptographic problem-solving known as "Proof of Work" to operate, many newer blockchains use "Proof of Stake" (PoS) systems that rely on market incentives. Server owners on PoS systems are called "validators" — not "miners." They put down a deposit, or "stake" a large amount of cryptocurrency, in exchange for the right to add blocks to the blockchain. In Proof of Work systems, miners compete with each other to see who can problem-solve the fastest in exchange for a reward, taking up a large amount of energy. But in PoS systems, validators are chosen by an algorithm that takes their "stake" into account. Removing the element of competition saves energy and allows each machine in a PoS system to work on one problem at a time, as opposed to a Proof of Work system, in which a plethora of machines are rushing to solve the same problem. Additionally, if a validator fails to behave honestly, they may be removed from the network — which helps keep PoS systems accurate."[15]

Additionally, proof of stake is elegantly simple in its architecture. Rather than requiring unfathomably complex machinery for solving an increasingly difficult algorithm, all that is required of stakers is skin in the game — a stake of the network's token that is put up for validation. Owing to the simplicity of proof of stake, there is less that can go wrong versus more complex systems, and much less required in terms of resources that strain the environment.

5.4 Bitcoin PoS Is More Secure Against 51% Attacks

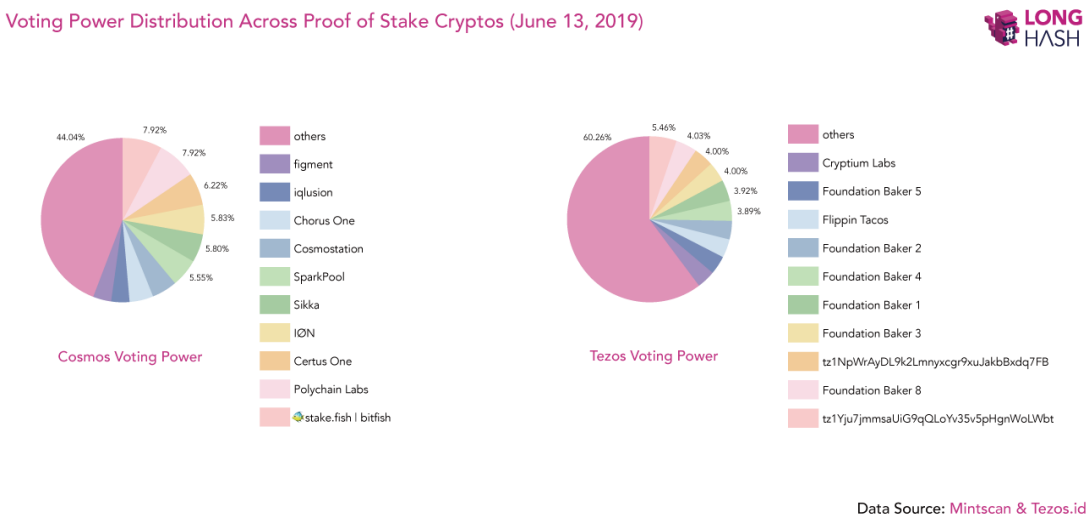
Security is the top concern amongst cryptocurrency advocates, investors, speculators, and network participants. Who wants to lose everything because of a flaw in the system?

Bitcoin has just such a flaw — it is called centralization. Mining creates a paradigm of centralization that raises the specter of a 51% attack. If such an attack were to occur, the entire network, and its billion of dollars in value, would be jeopardized. It's safe to say that in such a circumstance, the Bitcoin network would be finished.

Bitcoin PoS, by transitioning the entire updated Bitcoin codebase to proof of stake, avoids the possibility of a 51% attack with its elegantly simple design. Whereas an attacker needs to control 51% of the network hashrate for Bitcoin, if an attacker made an attempt on Bitcoin PoS, they would need to control at least 50% of the network's token supply.

This difference is very important to recognize. Hashrate can be consolidated by creating common interests for the heads of major mining cartels. However, tokens can't be consolidated by the same effort, since they are distributed across a wider cast of actors who have varying interests, aims, and network values. The effort required to sway token holders into selling or contributing their stake would be incalculably difficult, bordering on impossible, and so remains outside the scope of threats to Bitcoin PoS.

Staking pools, while beneficial for delegating stake and lessening the technical knowledge required by individual stakers, have been accused as possible sources of centralization within the proof of stake ecosystem. However, because staking pools don't require the physical warehousing of tokens being staked and are merely delegates of stake, don't possess the tokens in a saleable format. Again, this reduces risk of 51% network attacks for not only Bitcoin PoS, but all proof of stake networks.



Source: Longhash.com

6. Bitcoin PoS Architecture

At its core, Bitcoin PoS uses the same updated codebase as Bitcoin. The significant difference, however, is the consensus algorithm. Bitcoin PoS uses proof of stake, rather than proof of work, for consensus building.

It is important to note that Bitcoin PoS is not a Bitcoin chain fork. Instead, it is an original implementation of the Bitcoin codebase with several performance and consensus upgrades that make Bitcoin PoS a superior choice for financial applications such as payments — allowing to vastly improve network scalability.

Staking Prerequisites

Staking is the process of holding funds in a cryptocurrency wallet to support the operations of a blockchain network. Essentially, it consists of locking cryptocurrencies to receive rewards.

The following prerequisites apply to staking BPSs:

– The coins to be staked need to be matured; this means that the unspent outputs (UTXOs in short) need to have a depth in the main chain of at least the 500 blocks (which is the coinbase/coinstake maturity)

– The coins to be staked need to be in compatible address/transaction types (please check accordingly; at the time of writing this paper only P2PK and P2PKH are supported)

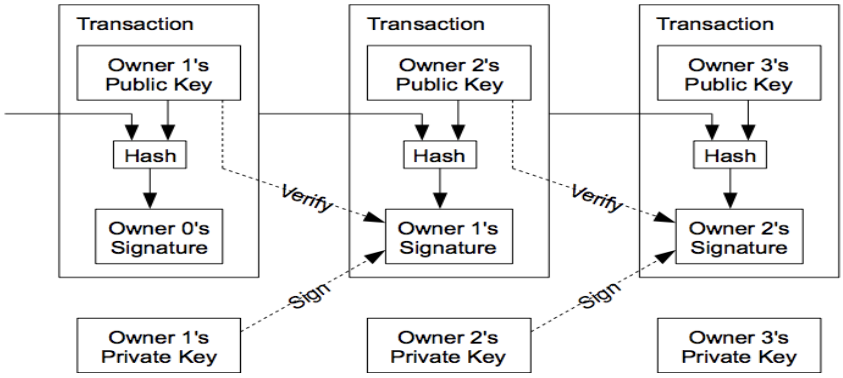
Block Structure

Bitcoin PoS uses PoS V3 as consensus algorithm. The blocks must abide by these rules:

- Must have exactly 1 staking transaction
- The staking transaction must be the second transaction in the block
- The coinbase transaction must have 0 output value and a single empty vout
- The block timestamp must have it's bottom 4 bits set to 0 (referred to as a "mask" in the source code). This effectively means the blocktime can only be represented in 16 second intervals, decreasing it's granularity
- The block's kernel hash must meet the weighted difficulty for PoS
- The block hash must be signed by the public key in the staking transaction's second vout. The signature data is placed in the block (but is not included in the formal block hash)
- The signature stored in the block must be "LowS", which means consisting only of a single piece of data and must be as compressed as possible (no extra leading 0s in the data, or other opcodes)
- Most other rules for standard PoW blocks apply (valid merkle hash, valid transactions, timestamp is within time drift allowance, etc)

Transactions

Like Bitcoin, Bitcoin PoS transactions function on the basis of public and private key signatures wherein a public key is verified, and a private key is signed by the sender.



In non-proof of stake blockchain networks, double spends are discouraged by the lack of incentive for staking every fork. However, proof of stake networks like Bitcoin PoS do incentivize staking every fork. Does this mean there is a higher chance of double spend transactions in PoS systems? The answer is no.

The above scenario is commonly referred to as the "nothing at stake" problem — but it incorrectly makes several drastic assumptions which are, in reality, nearly impossible. The most egregious of those assumptions is that every staker will stake every fork, when the possibility of amassing enough support per fork, no matter how far fetched, is nearly zero.

Because an attacker (or group of attackers) would need to incentivize stakers en masse to support a damaging fork, the logistics and cost of doing so are prohibitive.

In Bitcoin's proof of work algorithm paradigm, that isn't the case. Mining cartels aren't holding delegated coins, nor are they simply representing the interests of others. They possess unjustifiably large amounts of hashrate, making it possible for a double spend attack to occur should any of those heads of interest collaborate.

Therefore, Bitcoin PoS transactions are secure against double spend attacks while retaining the basic Bitcoin transaction infrastructure that users know and enjoy.

Mutualized Proof of Stake (MPoS) Consensus

Proof of stake consensus algorithms take on many forms. There are delegated proof of stake systems such as those used by EOS, and BFT PoS systems such as Cosmos. In the case of the former, dPoS adds undue complications to an already elegantly simple premise held by PoS networks. Additionally, dPoS algorithms introduce the possibility of increased network centralization, and don't create enough cost for an attacker.

To further prevent the possibility of an attacker disrupting the Bitcoin PoS blockchain, Mutualized Proof of Stake consensus function has been implemented. In a nutshell, MPoS creates an impossibly high cost barrier for malicious actors — one that is, theoretically, impassable.

Goals

1. Prevent malicious miners from attacking the network for free by constructing expensive to validate blocks, and then receiving all of the fees back to themselves through the mining process

2. Help to make it more difficult and expensive for an attacker to DoS the network

Procedure

1. When a staker mines a block, he receives only a small portion of the PoS reward and fees. The rest of the reward and fees are shared with 9 other people.

2. When a staker mines a block, his stake script (staketx.vout[0]) is registered to receive a share of the reward, lasting 10 blocks, 500 blocks from when the block was mined

3. Thus, every block there will be 10 reward recipients. The creator of the block, and 9 "mutual stakers".

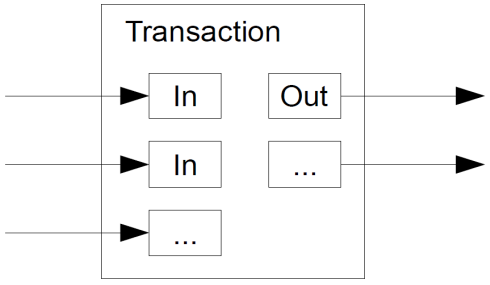
4. After 9 blocks of shared rewards, the staker's script will be removed, and another will be added to replace it

5. If a stake script has mined more than 1 block in a 10 block period, then there can be a case where he receives 2x the share. However, once the earliest stake script instance exceeds 510 blocks from it's mined block, it is dropped and the reward drops to normal. Identical stake scripts should not be combined into a single UTXO, the rewards should be duplicated

Under MPoS, attackers can't spam the Bitcoin PoS network with fees. Instead, network participants all share the fees, instead of the totality of fees going to a single block creator — as is normally the case. With fee sharing in place, and an ongoing rotation of stakers, the substance behind a spam attack vanishes. Additionally, because the MPoS algorithm has already been deployed at scale within our test network, its success under widespread use has already been proven.

Stake Aggregation

In order to eliminate practices such as transaction flooding whereby a staker can gain an advantage by staking with a high number of transactions (fan-out), Bitcoin PoS combines several inputs when creating the staking transaction (fan-in), trying to create a bigger stake for the block. To counter the unwanted effects of this input reduction mechanism which could lead to having really large trasanction outputs, if the stake is above a certain threshold it will also be split into several outputs.



Bitcoin PoS Payments

Of the many use cases prevalent for cryptocurrencies, the largest and most in demand is still payments. The world is slowly but surely transitioning to a paperless reality in which digital payments powered by similarly digital currencies are king — not cash.

Bitcoin cleared the way for this reality, but has stumbled in several major categories.

1. Bitcoin can not scale to the needs of millions — or billions — of worldwide users.

2. Bitcoin can't be easily integrated into existing payment rails and point of sale devices.

3. Bitcoin confirmations take far too long, making it inefficient for real time payments.

While some solutions, such as the Lightning Network, have been proposed and worked on, they are as yet missing from the space and have adoption issues of their own.

Bitcoin PoS has several advantages in the payments space. It is designed expressly for integration with existing payment systems, networks, and point of sale devices for a seamless cash to crypto experience. This transition is aided by wise design factors.

1. The small block size of Bitcoin systems is a scaling liability. Proof of stake blockchains such as Bitcoin PoS reduce block times to handle more transactions per second, making them fast enough to handle the speed of real time business.

2. Block finality in Bitcoin PoS is improved over Bitcoin which creates a major advantage for retailers and retail users as payments are settled nearly instantly and with finality.

3. Whereas proof of work scaling solutions take network activity off the main-chain and onto side-chains, Bitcoin PoS high throughput capabilities mean scaling is handled on the same chain — without having to rely on third party solutions.

Bitcoin PoS Coin Supply

Bitcoin PoS is not meant to compete with Bitcoin. Instead, it is meant to replace Bitcoin owing to its superior consensus algorithm, easily facilitated payments, and vastly reduced power consumption requirements.

Given these design goals, it is important to adhere strictly to the Bitcoin coin supply fundamentals, as Bitcoin PoS pushes for a strict adherence to Satoshi Nakamoto's original vision of a cashless, bankless, and third-party free financial experience.

Maximum Coin Supply — 21 million Bitcoin PoS (BPS)

Bitcoin PoS Block time

The Bitcoin PoS block time-spacing is set at 3 minutes, making it not only more than 3 times faster than Bitcoin, but also able to handle more than 3 times the number of transactions. The block difficulty is calculated using an algorithm that relies on exponential adjustments, and the difficulty is adjusted at every block. Using this algorithm makes block times more predictable and less prone to big spikes.

Bitcoin PoS Block Rewards

The Bitcoin PoS emission rate is similar to that of Bitcoin, with the key difference being that tokens are minted by stakers and the reduction rate is 25% every 700k blocks, starting with the block 120k, which occurs every 4 years.

The rewards for the the blocks up to 120k are split the following way:

- blocks 0 to 40000 have a reward of 50 BPS
- blocks 40000 to 80000 have a reward of 25 BPS
- blocks 80000 to 120000 have a reward of 12.5 BPS

At block 120001, the BPS and Bitcoin reward/block are aligned, at 6.25 BPS.

The blocks from 0 to 5000 are proof of work blocks, premined by the developers; these funds will be allocated for continued development and maintenance of Bitcoin PoS.

Apart from under-the-hood differences pertaining to consensus making and a vastly improved performance, the look and feel of Bitcoin PoS is strikingly similar to Bitcoin, and will make the transition for Bitcoin users simple.

Proof of stake offers rewards to stakers according to stake size. Just as with Bitcoin proof of work mining, where rewards go to the miner who solves the block (known as block rewards), Bitcoin PoS rewards also go to the staker, but split into 10 equal rewards (using the MPOS algorithm); the chance of minting a block is proportionate to the stake size, meaning, the higher the stake, the higher the chance is for the staker to mint a block before anyone else.

Bitcoin PoS collects fees from transactions and uses the fee amounts to reward stakers for the activity of securing/validating the network.

Source: [Ledger Academy]

Proof of work mining requires tireless commitment, expenditure of energy, high startup capital for investing hardware, and technical knowledge. Bitcoin PoS, on the other hand, can be staked in the background of other tasks, giving you the opportunity to earn passive income as a staker.

References

[1] https://blackcoin.org/blackcoin-pos-protocol-v2-whitepaper.pdf

[2] https://www.eia.gov/energyexplained/electricity/prices-and-factors-affecting-prices.php

[3] https://bitcoin.org/bitcoin.pdf

[4] https://www.forbes.com/sites/youngjoseph/2019/12/12/new-report-shows-china-dominates-bitcoin-mining-is-this-a-sign-of-worry/

[5] https://bitcoinmagazine.com/articles/op-ed-challenge-mining-centralization-unveils-bitcoins-elegant-design

[6] https://cointelegraph.com/news/bitmain-hits-15-billion-valuation-with-recent-backing-from-ubers-largest-shareholder

[7] https://cryptobriefing.com/bitcoin-mining-centralization-record-levels-majority-china/

[8] Ibid.

[9] https://www.nature.com/articles/s41558-018-0321-8

[10] https://www.forbes.com/sites/andreamorris/2018/10/29/bitcoin-predicted-to-be-the-nail-in-the-coffin-of-climate-change/#47a1917e745e

[11] https://www.theverge.com/2019/7/4/20682109/bitcoin-energy-consumption-annual-calculation-cambridge-index-cbeci-country-comparison

[12] https://www.binance.vision/security/what-is-a-51-percent-attack

[13] https://cointelegraph.com/news/the-dangers-of-mining-pools-centralization-and-security-issues

[14] https://bitcoinist.com/ethereum-pos-blockchain-cut-energy/

[15] https://hbr.org/2018/11/making-cryptocurrency-more-environmentally-sustainable