BitcoinStaking: A Peer-to-Peer Electronic Cash System

BitcoinStaking Developers
support@bitcoinstaking.org
www.bitcoinstaking.org

1. Introduction

BitcoinStaking (BitcoinS - BSK) is the world's first integration of cryptocurrency's two foremost technological accomplishments — Bitcoin, and proof of stake (PoS) consensus. Today, Bitcoin core continues utilizing proof of work (PoW), a consensus algorithm that has many flaws such as vulnerable to 51% attacks, costly to mine, and detrimental to the environment. Bitcoin does contain many unique innovations that require preservation, such as its 21million coin supply model and proven code-base which has had countless foremost software engineers and cryptographers continuously scan its codebase fixing any vulnerabilities that may arrise. By combining Bitcoin's strongest assets with a highly efficient, scalable, and flexible PoS consensus algorithm, BitcoinStaking introduces a new shift for how cryptocurrency's transactions function. BitcoinStaking does everything Bitcoin is currently able to do, while adding new advances in blockchain technology, thereby updating crypto for the future.

2. Mission

The world continously thirsts for better ways gain trust in cryptocurrency. Bitcoin has Kicked off a cryptocurrency revolution that hasn't been adopted by the masses. Many cryptocurrency projects have failed everyday users by under-delivering on promises and dumping their assets for profit. BitcoinStaking aims to pick up where Satoshi Nakamoto's vision of a decentralized virtual cloud based baking system and peer-to-peer electronic cash system left off. BitcoinStaking is easy to use, scalable or the masses, secure — and easy to adopt for enterprise, people, and retail applications.

3. What is Proof of Stake?

Bitcoin consensus is achieved by requiring generated blocks to contain a proof that the miner that created the block solved a computationally difficult task. As we now know, unfortunately the Proof-of-Work(PoW) based systems tend to spiral towards self-destruction. For instance, if a new ASIC miner comes out with abilities of 1Million times the current miners, it could render Bitcoin frozed forever.
Proof-of-stake (PoS) replaces the way consensus is achieved in a distributed system. Rather than solving the PoW, the staker that generates a block must provide a proof that It owns a certain amount of coins before being accepted by the network. Generating a block involves sending coins to oneself; this proves ownership and in doing so the staker can create a new block that has other transactions in it as well. The required amount of coins (also called the “stake”) is specified by the network via a difficulty adjustment algorithm similar to PoW that ensures a loose way to obtain 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 by a period of PoW mining.

4. Bitcoin is Centralized

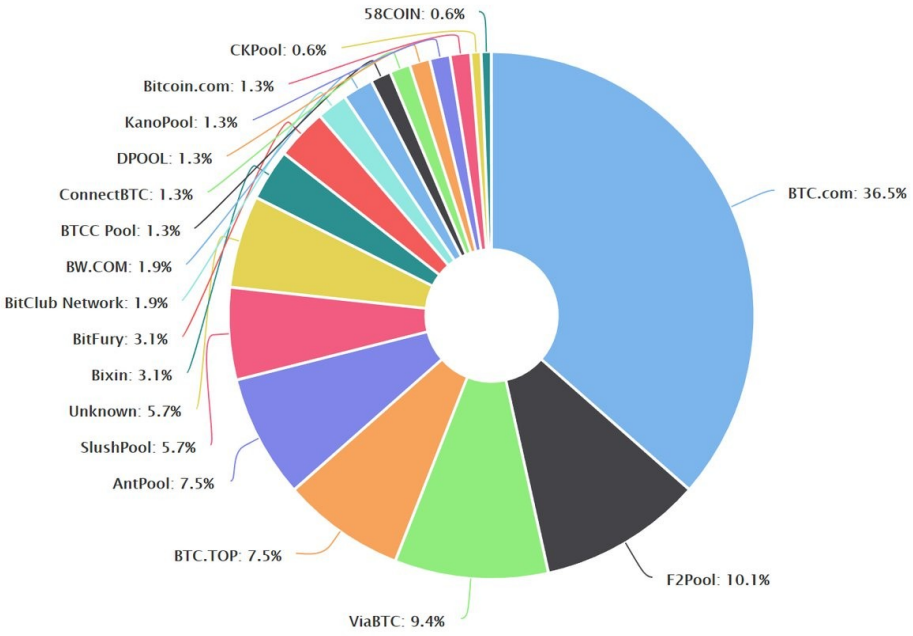
Many Bitcoin defenders say that Bitcoin isn’t broken, however that view quickly goes out the window when looking into the future. Dependent on its high power electricity-based Mining dependent architecture, Bitcoin has little incentive to promote centralization of the world’s mining resources. Additionally, mining Bitcoin requires that one possess the required mining resources; however the large corporations tend to mine with their latest technology miners before allowing the general user to get their hands on them.

4.1 PoW means lots of Electricity

The largest concern of any Bitcoin miner is the cost of electricity and the cost to replace an expensive ASIC miner if it breaks. China remains at the top of Bitcoin mining centralization due to electricity costs around the world not being uniform. What results are electricity bottlenecks in which some geographic regions rise above others. This allows miners in regions with cheaper available electricity to monopolize the Bitcoin mining industry. Monopolization means centralization, the “evil” that Satoshi Nakamoto hoped would vanquish in the original Bitcoin whitepaper. To add to the problem, governments in countries where electricity costs are elevated have not recognized the Bitcoin mining industry in any way, meaning benefits of tax write-offs are out the door. Given the involuntariness of governments to help in subsidizing electricity costs to benefit the decentralization of Bitcoin technology, there is no clear cut solution to the growth and profiteering of the mining cartels, the bulk of which live in China. Bitcoin has no mechanism in place to reward decentralization. Due to the nature of PoW, those who create the largest mining facilities with access to cheap electricity can outmatch, out-mine, and financially profit above and beyond smaller miners. The every day, small mom and pop miners were once the hope of maintaining a balanced Bitcoin network.

4.2 Bitcoin PoW Centralization will lead to a 51% Attack

Another drawback to the PoW centralization of Bitcoin is security. Centralization of the PoW mining process allows for the network to become susceptible to double spend attacks. The possibility of the famed 51% attack is growing day by day. Basically, a 51% attack refers to the possibility that a group of miners could concentrate and form a majority of the Bitcoin network's hashrate. This in itself is not the real problem. The real problem is when the majority has ill intent, thus intentionally falsifying transactions for the greedy benefit of being able to erase transactions and obtain the Bitcoin again; this is double spending. Many believe that a 51% attack of the BTC network is unlikely, but really they are hoping It never happens because the price will collapse like a falling knife. This would lead to the community to distrust Bitcoin and it would never recover to what we know today. A 51% attack would be so devastating to Bitcoin that it would 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:

5. BitcoinStaking PoS Solves Bitcoin's Centralization Problem

The problems associated with Bitcoin’s centralization are many and have been documented in the foregoing sections. However, BitcoinStaking 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. BitcoinStaking 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 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. BitcoinStaking 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%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 BitcoinStaking PoS network can simply use the energy source from wherever they are. The electricit 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 BitcoinStaking Makes Staking Easy

Proof of work networks require miners with access to cheap electricity and expensive hardware mining rigs. 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 BitcoinStaking PoS coins in their wallet.

Reducing the burden on network participants is a key BitcoinStaking 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 BitcoinStaking to encourage mass participation.

5.3 BitcoinStaking Is More Secure Against 51% Attacks

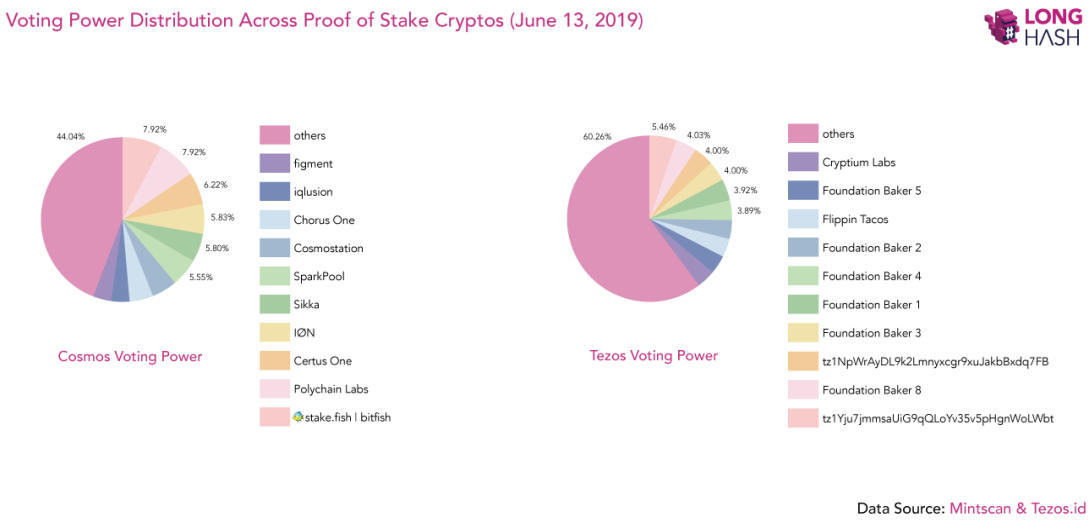
Security is the top concern amongst cryptocurrency advocates, investors, speculators, and network participants. Who wants to lose everything because of a flaw in the system?

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.

BitcoinStaking, 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 BitcoinS, they would need to control at least 50% of the network's coin 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 BitcoinStaking.

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 BitcoinS, but all proof of stake networks.



Source: Longhash.com

6. BitcoinStaking Architecture

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

It is important to note that BitcoinS is not a Bitcoin chain fork. Instead, it is an original implementation of the Bitcoin codebase with several performance and consensus upgrades that make BitcoinS 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 BSKs:

– 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)

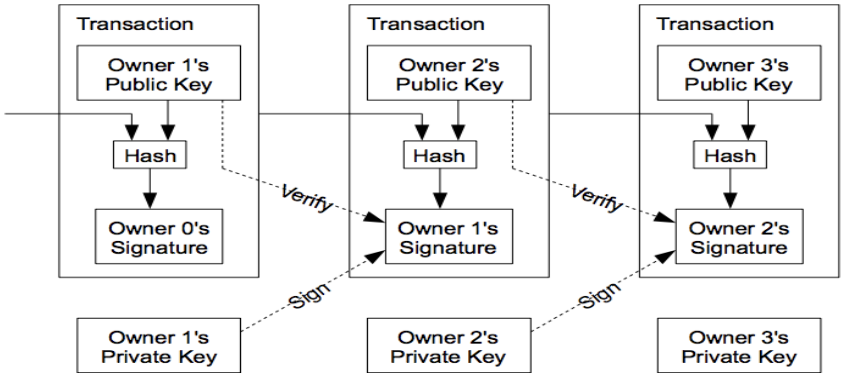
Block Structure

BitcoinS 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, BitcoinS 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 BitcoinS 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, BitcoinS 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 BitcoinS 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.

MPoS Explained

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".

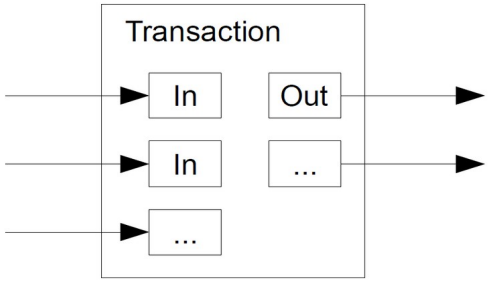
4. After 9 blocks of shared rewards, the staker's script will be removed, and another will be added to replace it

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 BitcoinS 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), BitcoinS 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.



BitcoinStaking Coin Supply

BitcoinS 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 BitcoinStaking 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 BitcoinStaking (BSK)

BitcoinS Block time

The BitcoinStaking block time-spacing is set at 10 minutes.
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.

BitcoinS Block Rewards

The BitcoinS emission rate is much slower than Bitcoin, with the key difference being that tokens are minted by stakers.

The rewards for the the blocks up to 6000 are split the following way:

– blocks 0 to 5000 are PoW and have a reward of 50 BSK

– blocks 5001 to 6000 are PoS have a reward of 50 BSK

At block 6001 and onward, all block rewards are 1 BSK until 21 Million BSK Have been mined.

The blocks from 0 to 6000 are premined by the developers; these funds will be allocated for continued development and maintenance of BitcoinS.

Apart from under-the-hood differences pertaining to consensus making and a vastly improved performance, the look and feel of BitcoinS 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), BitcoinS 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.

BitcoinS 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. BitcoinS, on the other hand, can be staked in the background of other tasks, giving you the opportunity to earn passive income as a staker.