



**Bitcoin Staking (BSK)**

**W H I T E P A P E R**

# ***The Revolution of Decentralization***

*Fulfilling Satoshi's Vision for 2020 and Beyond*

*October 2020*

*Authors:*

***Unnamed Furious***

***Fluffy Dragon***

***Hitoshi Konami***

**WWW.BITCOINSTAKING.ORG**

# ***Table of Contents***

1. Introduction
2. Fork Methodology
3. Proof-of-Stake
4. Is there a premine?
5. PoS Reduces Electricity Consumption by 99.999999999%
6. Bitcoin Staking PoS Solves Bitcoin's Centralization Problem
7. Bitcoin Staking Makes Staking Easy
8. The mission

## ***1. Introduction***

Bitcoin Staking (BitcoinS - BSK) is the 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 arise.

Bitcoin Staking (BSK) is the ultimate solution for the above issues. By transitioning from a proof of work (PoW) to a proof of stake (PoS) algorithm, BSK protocol as improvement will lead to further and wider achievements in decentralization and energy consumption. Bitcoin Staking has released the first ever BTC PoW to PoS consensus transition, giving the growing option to the Bitcoin network to transition to proof of stake. Ethereum has transitioned to PoS and now Bitcoin has transitioned to proof of stake via BSK.

## ***2. Fork Methodology***

BSK is the first Pure Proof of Stake (PPoS) hard fork of Bitcoin; it was created by staking real BTC; this makes BSK a pure PoS transition from BTC PoW. You can mine BSK using real 2014 BTC keys with a balance or from staking BSK in your wallet.

BSK is a fork of Bitcoin at block 301448 (May 2014). Block 301447 is the last PoW block and all Bitcoin keys (@block 301447) transfer to the BSK chain as it is a fork of BTC. Block 301448 is the first block that uses PoS. Block 301448 was chosen because that marks the point in which about 60% of all BTC has been mined. This gives a good coin supply for staking in the future as well as allowing another 40% to be mined by future PoS Bitcoiners.

### ***3. Proof-of-Stake***

Bitcoin Staking consensus is achieved by requiring generated blocks to contain a proof that the miner that created the block solved a computational 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 frozen for a very long time. 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. 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 BSK distribution of the currency is from old Bitcoin addresses that used PoW mining.

#### ***4. Is there a premine?***

Satoshi created the first block and mined many other blocks back in 2009. Starting with Block 301448, BTC addresses from 2012 through 2014 have been used to continue PoS mining beyond block 301447. This means that there is NOT a premine; only a continuation of PoS mining using old BTC keys.

## ***5. PoS Reduces Electricity Consumption by 99.999999999%***

BSK uses a Proof of Stake algorithm. The solution for the PoS algorithm is based on randomness in time and prior block bits. Using a mathematical formula that has the user's coin amount as a scale factor to determine acceptance allows easy cpu computations every few seconds rather than using ASICs at supersonic clock rates. The user's coins are essentially the equivalent of the amount of ASICs a mining farm has. The BSK wallet/node running on a PC uses virtually no power compared with ASIC miners.



## ***6. Bitcoin Staking PoS Solves Bitcoin's Centralization Problem***

The problems associated with Bitcoin's centralization are many and have been documented. However, Bitcoin Staking 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 Staking 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.

## ***7. Bitcoin Staking 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 Bitcoin Staking PoS coins in their wallet.

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

## ***8. The mission***

Very simply, we encourage the original Bitcoiners to use their old addresses and start staking on Bitcoin Staking. BSK is everything Bitcoin is plus Proof of Stake. Legacy Bitcoiners can easily contribute to the BSK mining process by downloading a wallet and importing their keys. Immediately we will have a Bitcoin Proof of Stake blockchain that is much safer from 51% attacks than the PoW blockchain. Think about this, what would happen if the power went out at one or two major BTC ASIC farms? A opportunity would exist for 51% attack. Now what would happen if a few whales turn off their wallet on BSK? Not much, since everyone participates by simply leaving their BSK wallet on, the BSK network would continue to operate in a safe manner because many more miners are controlling the BSK network because it is much more feasible for an average person to run the BSK wallet on a laptop than buy and operate an ASIC.

Come join the BSK community and turn Bitcoin into a Proof of State blockchain!

**Please move your BTC to another safe address before importing your keys!**