BitcoinV PoS: A more decentralized form of Bitcoin

NullFunctor
github.com/bitcoinVBR
www.bitcoinv.org

Abstract. Satoshi Nakamoto's original vision for Bitcoin was to create a peer-to-peer version of electronic cash. The majority of successful forks of the protocol try to improve on this vision further and provide a more scalable and efficient system for payments. We see Bitcoin's greatest promise not as a medium of exchange but as a store of value – a better form of gold, not cash. We propose a set of modifications to the original protocol aimed at fulfilling this promise by creating the ultimate electronic store of value. By increasing Bitcoin's mining decentralization, we are able to tackle Bitcoin's greatest flaw as a form of gold – mining centralization.

1. Introduction

Bitcoin is an innovative decentralized payment system launched in 2009 allowing parties to transact directly without going through a trusted financial institution. The system relies on proof-of-work to maintain a distributed ledger without a trusted operator, that is secure as long as honest nodes control more CPU power than any cooperating group of attacker nodes. Bitcoin was originally described by its creator Satoshi Nakamoto as an "electronic cash system".

Multiple successful modifications of the original protocol have been released over the years in the form of forks of the Bitcoin codebase. These include Litecoin that launched in 2011 to reduce transaction confirmation time and change the proof-of-work algorithm to favor consumer-grade hardware such as GPU; Bitcoin Cash that launched in 2017 to scale the original protocol's transaction throughput by increasing block size; and Bitcoin Gold that also launched in 2017 to render specialized mining equipment obsolete by changing the hashing algorithm.

True to the original vision, the primary focus in these forks and others is to make Bitcoin a better system of cash. Limitations of the original protocol such as high transaction fees, 10 minute confirmation times and approximate throughput of only 4 transactions per second hinder Bitcoin's ability to compete with the centralized online payment systems dominant today.

2. Electronic Cash or Electronic Gold

Whereas Bitcoin did not see much success with consumer adoption as electronic cash, it has been significantly more successful as a form of electronic gold. There is a long standing industry debate whether Bitcoin is superior as a medium of exchange or in fact as a store of value. Gold is not an effective means of payment for day-to-day goods and services. Consumers primarily invest in gold to hedge against inflation and preserve future purchasing power. Unlike national currencies, Bitcoin's fixed monetary policy and limited supply make it particularly attractive in this regard.

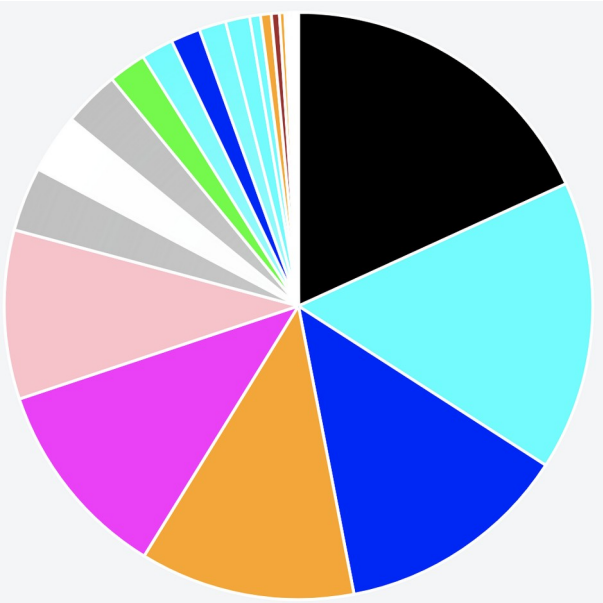
History shows that systems can rarely be designed to meet several competing goals at once. Optimizing Bitcoin to become a better medium of exchange diminishes its potential as a store of value. On the same note, by sacrificing further on the properties required for useful electronic cash, we can vastly improve its utility as electronic gold. In this paper, we propose a series of modifications to the original Bitcoin protocol focused on a single goal – creating the ultimate store of value.

If we no longer prioritize competing as an online payment system, we need not focus on transaction fees or transaction throughput. After all, gold is expensive to transport and is normally acquired for long term investment. A property that is particularly relevant to our efforts is transaction confirmation time. tradeoffs on this front, such as substantially increasing Bitcoin's average 10 minute confirmation time, can yield cardinal advantages. Since we would not expect to freight a shipment of gold across locations in under 10 minutes anyways, this sacrifice seems natural.

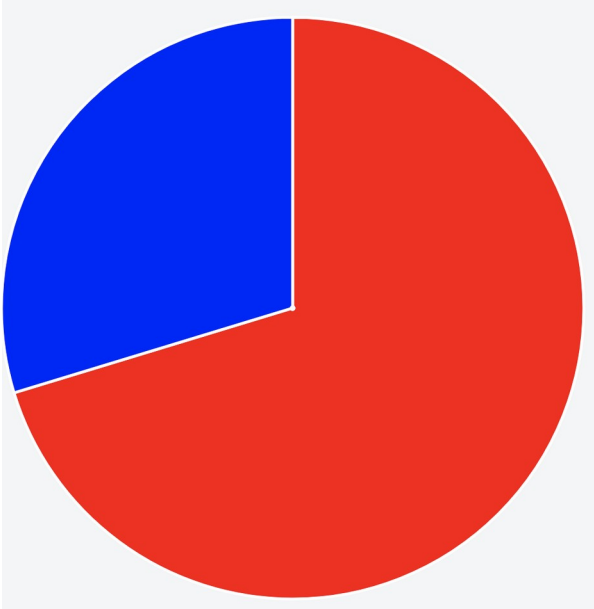
3. The Problem of Centralization

Bitcoin was originally designed to be decentralized, through its journey it didn't end up following this path and never will. Some say because Bitcoin has become centralized that it is doomed and is on a death spiral, however give the world a large enough incentive and decentralization can surface back to life bringing the new Bitcoin back to Satoshi's original vision of staying decentralized.

Pictures are worth a thousand words, take a look at the charts below. (Keep in mind that 51% of the hashing assumes the power to do something) The chart below shows the distribution of hashing power for Bitcoin (Mid 2018). Technically, one needs to hijack 3 to 4 entities to gain control of the hashing power. Let's pretend AntPool, BTC.com, ViaBTC, F2pool, BTCtop are independent non-colluding organizations and not just one entity hiding to be 5. GHash failed because they publicly demonstrated owning 51%. Chinese miners have learned from this and are smarter than publicly showing a 51% ownership.
The chart below shows how nicely the hash rate is divided with no clear leader. The distribution is still heavily centralized due to the accumulation of the 4 largest slices of the pie forming a centralized entity with over 51% hashing power. In general countries have the authority over miners residing in their country.



Here is what happens when we compare China vs. non-China with regards to Bitcoin hashing power.



Clearly this is a threat to the Bitcoin community. Over 51% of the hashing power resides in China.

4. Solution – Proof of Stake with Variable Block Recipients (VBR)

BitcoinV PoS solves the mining centraliztion problem by preventing ASICs to scale and mine on the network. The Proof of Stake nature of BitcoinV only allows wallets (with coin) to mine on the network. The more coin the wallet holds, the higher probability that the wallet will mine the next block. In addition to the PoS, BitcoinV adds the Variable Block Recipients (VBR) feature for more decentralization

To further prevent the possibility of an attacker disrupting the BitcoinV blockchain, Variable Block Recipients (VBR) algorithm has been implemented. In a nutshell, VBR creates an impossibly high cost barrier for malicious actors — one that is, theoretically, impassable.

Goals of VBR Staking

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

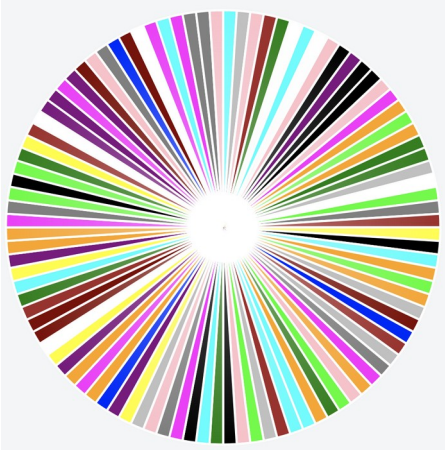
Procedure

1. When a staker mines a block, they receive 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. Every block there will be 10 reward recipients. The creator of the block, and 9 "Variable Block Recipients".
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

Since the Variable Block Recipients (VBR) algorithm gives a small portion of the PoS reward and fees to the miner, the rest of the reward and fees are shared with 9 other users. This discourages users from loading up on coin just for the sake of trying to dominate the staking rewards because when they stake, they only get one tenth of the reward and fees. This discouragement is what makes the VBR feature allow for more decentralization. Naturally as the coin spreads across more wallets, more decentralization is achieved

5. Decentralization Expectations

As the BitcoinV community grows and the mining becomes mature, the expectation is that many miners will form around the world playing for the large as well as other variations of block reward payouts. Once this happens, the world distribution can look like the following chart.



5. Block Rewards and Premine

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

Max supply: 42 Million BTCV
Block time: 10 Minutes
Block reward: Fixed at 10 BTCV

The rewards for the the blocks up to 7000 are split the following way:
– blocks 0 to 5000 are PoW and have a reward of 2000 BTCV
– blocks 5001 to 7000 are PoS have a reward of 2000 BTCV
At block 7001 and onward, all block rewards are 10 BTCV until 42 Million BTCV have been mined.

The blocks from 0 to 7000 are premined by the developers; these funds will be allocated as follows:
- 7 Million BTCV for swapping all users and exchanges holding old BTCV.
- 7 Million BTCV for the dev team for listing on future exchanges, paying bounties, and continued development and maintenance of BitcoinV PoS.