BitcoinV: A more decentralized form of Bitcoin

NullFunctor
github.com/bitcoinVBR

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 [2] 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 [3] 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 [4] that launched in 2017 to scale the original protocol's transaction throughput by increasing block size; and Bitcoin Gold [5] 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.

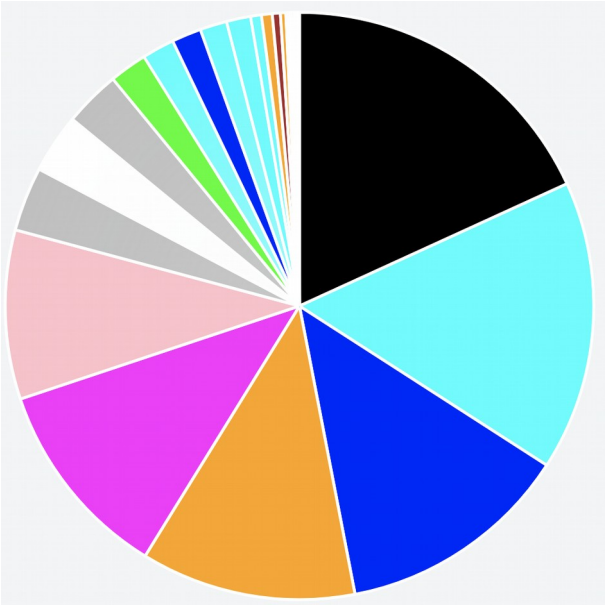
History shows that systems can rarely be designed to meet several competing goals at once. Optimizing Bitcoin to become a better medium of exchange diminishes its potential as a store of value. On the same note, by sacrificing further on the properties required for useful electronic cash, we can vastly 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.

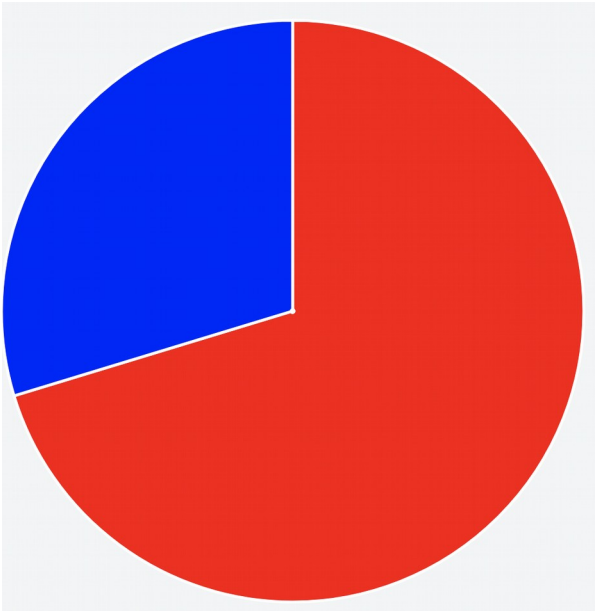
3. The Problem of Centralization

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 - Variable Block Rewards (VBR)

There are ways to solve this problem, some easier than others. A difficult solution is to reduce the amount of miners controlled by China. The easier solution to this problem is to spread out the miners throughout the world. BitcoinV follows the easier solution by providing incentive for miners to start mining throughout the world.

BitcoinV uses a similar algorithm as Bitcoin to determine difficulty level and its corresponding difficulty level adjustments over a 1-block interval. The VBR feature itself is an algorithm add-on that gives addition rewards for miners who can have the least significant bits (lsb) of the block hash match those of the Merkle root in the same block. The more bits that match, the more the reward. Miners must prove their intent in order to get the reward. For instance, if a miner's intent is to grab the regular reward of 50 BTCV and they happen to match additional bits, the payout is still the standard reward of 50 BTCV.

Example:
If a miner shows his intention of trying to mine for a 64 * standard block reward, the miner would signal this by creating a coinbase transaction of 64*50 = 3200 BTCV. The requirement to successfully mine the block is to satisfy the original Bitcoin difficulty level as well as satisfy the VBR requirement of matching 6 (lsb) (2^6=64) of the current block's hash and the Merkle root that resides in the current block. If both are satisfied, the blockchain accepts the block and the miner is rewarded 3200 BTCV.

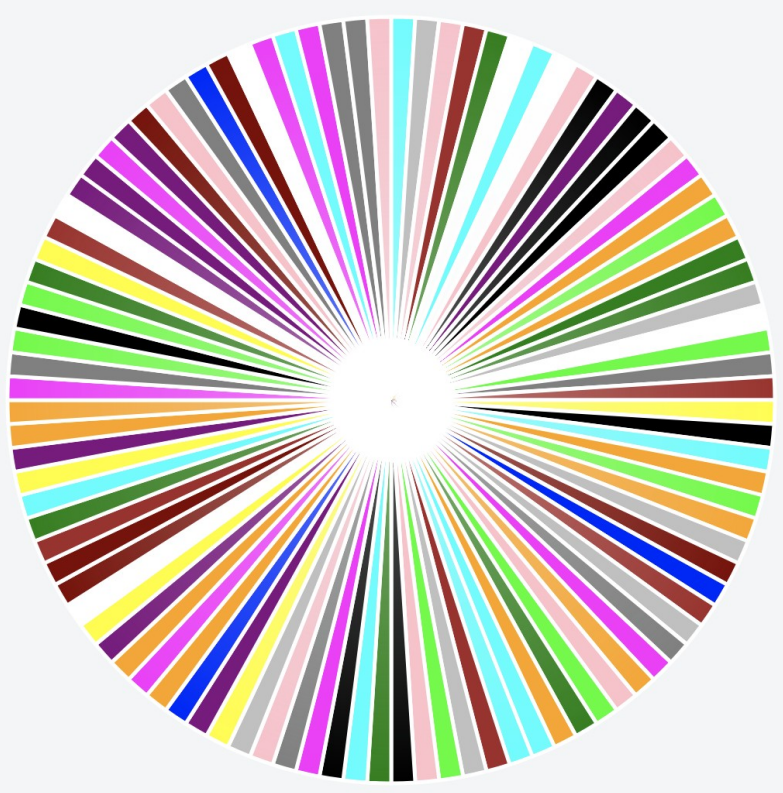
Take for instance, using the example above, if the miner (going for 3200 BTCV) only satisfies the original Bitcoin difficultly level requirements, the block would be rejected; too bad for the miner because if he chose the 50 BTCV reward, he would have had his block accepted. But this is the risk a miner must take to try and mine the large block reward.

Many miners in general would prefer to go for the larger rewards. In doing so, they need to work harder to find a block that will get accepted. This creates the impression to the original Bitcoin difficulty algorithm that it is too hard to find a block and the difficulty level would then decrease. This however is not completely realistic because some miners will also mine for the minimum block reward which will be found faster thus keeping the difficulty level still difficult to protect against rewriting the block chain.

Hope is the most personally detrimental human emotion that we know. Hope is what will drive solo miners to try and mine larger block rewards and make BitcoinV a more decentralized form of Bitcoin. This is human nature.

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.



References

1. NullFunctor https://medium.com/@support_43415
2. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, https://www.bitcoin.org/bitcoin.pdf, 2008.
3. Litecoin Project, “Litecoin, open source P2P digital currency”, https://litecoin.org, 2014.
4. “Bitcoin Cash”, https://www.bitcoincash.org, 2018.
5. bitcoingold.org, “Bitcoin Gold”, https://bitcoingold.org, 2018.