BitcoinV: A Bitcoin System with Variable Block Rewards

NullFunctor
www.bitcoinV.org

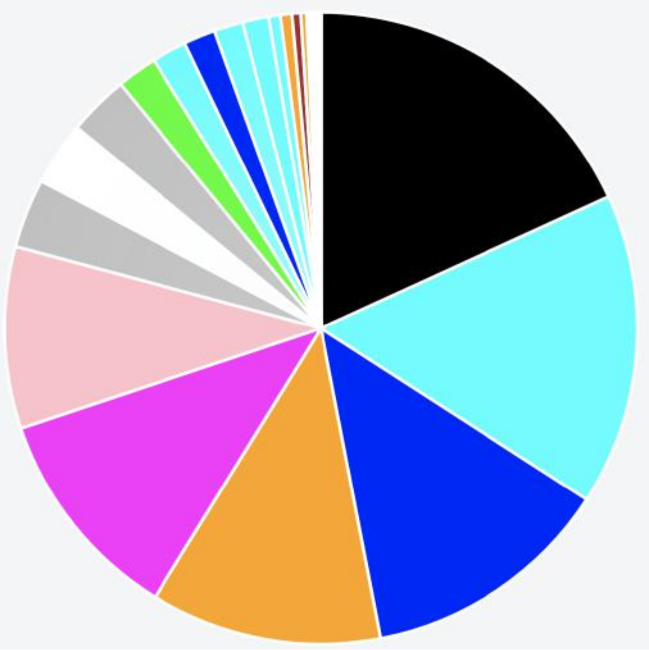
1. Introduction

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, I give you BitcoinV!

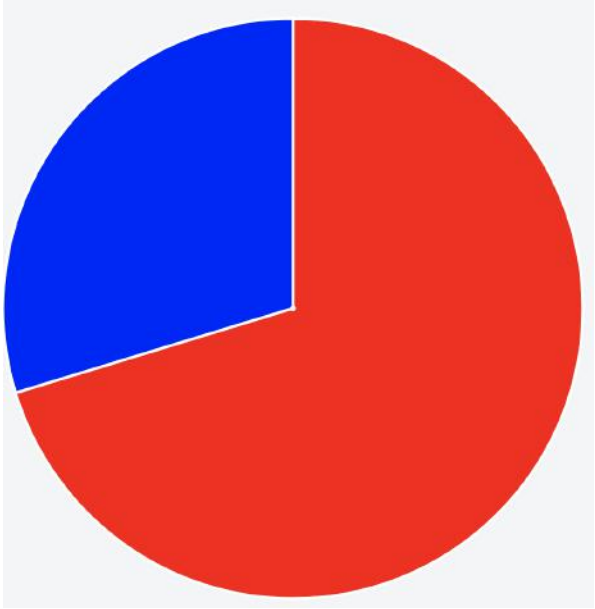
Pictures are worth a thousand words, take a look at the charts below. (Keep in mind that 51% of the hashing assumes the power to do something)

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.

Solution

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. Under the current Bitcoin system, simple CPU and GPU miners do not even bother to participate because they will most likely never find the nonce to solve a block and reap the 12.5 BTC rewards that come with it.

Under the BitcoinV blockchain, CPU/GPU miners would have an incentive to participate because they can choose to mine for a block with a larger block reward. There are JACKPOT block rewards that payout 1,000,000 times the current block reward. Now, many more CPU/GPU miners would turn on there miners throughout the world knowing that they may hit the “Big One” and get BTCV rewards in the millions.

Variable Block Rewards (VBR)

BitcoinV uses the same algorithm as Bitcion to determine difficulty level and its corresponding difficulty level adjustments over a 2-week 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 128 * standard block reward, the miner would signal this by creating a coinbase transaction of 128*50 = 6400 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 7 (lsb) (2^7=128) 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 6400 BTCV.

Take for instance, using the example above, if the miner (going for 6400 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. There is a reason for this. If ASIC miners kept trying to go for the JACKPOT reward, they would almost always keep winning the standard reward and never let the CPU/GPU miners play for any type of reward.

ASIC 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 ASIC 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.

JACKPOT Block Rewards

Jackpot block rewards are rewarded when the miner signals his intention of playing for the JACKPOT, this is accomplished by creating a coinbase transaction of 2^20 (about 1 million). The blockchain will only accept this block if 20 lsb bits match between the Merkle root and the hash AND the original Bitcoin difficulty level is satisfied. A nice feature of VBR is that one does not have to only play for the JACKPOT. A miner can choose to play for the minimum reward or any VBR between 1 and 20 bits matching.

As one can imagine going for the JACKPOT reward has the feeling of playing the POWERBALL or MEGA-MILLIONS and hoping to hit the JACKPOT, yes it does happen and this is why people all over the world keep playing the LOTTO. Along the same lines, this is why people all over the world will become a part of BitcoinV and create a decentralized blockchain.

BitcoinV: Decentralization Expectations

As the BitcoinV community grows, the expectation is that many CPU/GPU miners as well as ASIC miners will form around the world playing for the JACKPOT as well as other variations of block reward payouts. Once this happens, the world distribution can look like the following chart.

Thank you for reading the BitcoinV whitepaper. If you would like to join the community, please go to:

http://www.bitcoinv.org

and download the Window's miner:

https://github.com/bitcoinVBR/bitcoinV/releases/download/latest/bitcoin-qt.exe