BURST

Burstcoin.info blog

Jun 07 2015 by Matthew Czarnek

Why Proof of Capacity should be taken seriously

Technical details and proofs of numbers stated here are coming soon in future posts, however this is an overview of the advantages of Proof of Capacity as a mining algorithm.

In the minds of many people involved in cryptocurrency there are two mining algorithms: Proof of Work and Proof of Stake. Amazingly though and luckily for me and anyone else finding Burst at its current ridiculously low market cap, most people haven't heard or seriously considered one other major algorithm that has more potential than either of the other two, Proof of Capacity.

The first reaction many people have is if you are looking for a new algorithm, then why not go for a variation of Proof of Stake? It seems like the obvious choice; you totally eliminate the energy hungry mining equipment from the equation. However, Proof of Stake has a few key issues with it. And those who realize those issues, assume that Proof of Work is the only algorithm with potential.

First, let me quickly explain how the various Proofs work. All blockchain algorithms work by linking together blocks that contain all the transactions that occurred during a certain block of time. Miners are paid because these blocks contain transaction fees, as well as initial transactions. All transactions occur similarly in all these networks, however it's the way that these blocks are linked together which is the issue at hand.

In a Proof of Work network, everyone hashes the last block plus a random number they have created until they find a valid hash that meets certain criteria. These hashes prove that a whole lot of work has been spent creating the block and therefore the miner who created it must have spent a lot of money on his mining equipment.

In a Proof of Stake network, the mining equipment is not important. The miners get to mine approximately the portion of blocks that correspond to the percentage of the coins they control.

With Proof of Capacity the portion of blocks a miner gets to mine corresponds to the amount of hard drive space that miner has dedicated to mining for the network. At first glance, it seems approximately the same as Proof of Work, using hard drives instead of mining equipment.

Again, I will go into more detail and prove these numbers in future posts but there are calculations to back them up. This is just a quick overview.

Proof of Capacity has several advantages over both Proof of Work and Proof of Stake.

Proof of Capacity vs Proof of Work

Energy Efficiency

The biggest reason that Proof of Capacity beats Proof of Work is that Proof of Capacity is very energy efficient, using approximately 30 times less energy per dollar spent than for a Proof of Work miner. This is a fair comparison because miners will spend a certain amount of money in order to attain a certain ROI given a similar network that has similar transactions and block rewards.

Ease of Mining for Everyday People

Mining for a Proof of Work coin requires an ASIC to mine. ASICs are expensive, loud, energy consuming, and in some cases require extra cooling systems. This is not something an average person is going to buy but everyone already has a hard drive.

Being ASIC Proof means that every day people can mine for the network and be just as efficient as the people who buy fancy, expensive equipment trying to gain an edge over each other. because those people will also be buying hard drives and any technology that allows easy mining will also offer an edge to businesses and people that require cheap storage technologies and most people also should own such equipment if they regularly backup their computer as is highly recommended.

If you look at Litecoin, back when it was ASIC resistant, though not ASIC Proof as Proof of Capacity appears to be, you'll see that there was a huge rush

of people buying extra graphics cards to mine for Litecoin. Odds are that Burst will create similar rushes, and lead to people buying extra hard drives. At the moment, your average miner mines with 12.5 TB if you analyze the miners for Burst.ninja. Which seems likely to remain steady as new miners join in on securing the coin.

Proof of Capacity vs Proof of Stake

Energy Efficiency

Proof of Stake does use a little bit less energy but Proof of Capacity only uses approximately 25% more energy as Proof of Stake for a similarly sized network due to the low energy usage of hard drives compared to the attached computer that has to be used to mine in an equally sized and decentralized Proof of Stake network.

Blockchain trimming

Proof of Stake has some serious issues when it comes to trimming its blockchain. In a Proof of Work or Proof of Capacity environment, you can take these Proofs and use them to prove that a given chain of blockchain headers is valid. In Proof of Stake, these blockchain headers are made using Proofs that rely on the blockchain to be created. Ethereum has proposed a blockchain trimming solution but it is risky and flawed as it relies on at least 66% of miners staying online at all times. In a later blog post I will show why this is flawed and will not work.

Proof of Stake Cannot be as Trustless

In a Proof of Work or Proof of Capacity system, you can find a blockchain that has had more work than the rest used to create it. And you can show that these miners have agreed on which chain is correct. In a Proof of Stake coin, there is no way to prove that you are mining on the correct chain in a trustless manner.

The only plan I've heard so far that could help is to have corporations such as Walmart and McDonalds essentially 'vote' on which chain is correct and then rely on the majority to win. This is the so called 'Economic Clustering' Nxt has discussed. So essentially, we're trusting corporations to secure the blockchain. which seems to conflict with the goals of most of the people interested in cryptocurrency. And because this type of agreement is susceptible to the Byzantine Generals problem, it means that we have to trust that over 2/3rds of the agreeing parties are honest. With those votes, this leaves the chain with both

a 51% attack on the blockchain as well as a 33% attack on the number of votes. This method is much more complicated both for developers to write as well as customers to use and harder to prove correct.

The other way to achieve some trust lessness that helps this problem of determining the correct genesis block is to add Proof of Work to the equation, similar to what Peercoin does where Proof of Work is initially used to create the coins, but then it is tapered off and replaced with Proof of Stake. But in this case, that trust lessness about which genesis block is correct is only as strong as the Proof of Work component, leaving the coin wide open for 51% attack on the Proof of Work component by creating fake chains and with the Proof of Stake component not providing any extra protection against this type of attack.

Proof of Stake Relies on Miner's Keys Remaining Secret

Two issues with miner's keys potentially being compromised:

1)In order to mine a miner must store his private key on a computer mining for the network connected to the internet. This directly contradicts the idea of best practice security for cryptocurrency in general where holders should hold on to their keys offline and in a secure location.

2)History key attacks are possible where miners sell their private keys long after they have emptied their accounts and the key is otherwise useless. Proof of Stake supporters have argued that this is not a problem because of decentralized checkpoints not allowing the blockchain to be rolled back far enough for this to occur. The attack vector that this miss is that such an attack could happen using forks off of blocks over a year which ends up with millions fake forks building off of various blocks, and how can a new miner just joining the network for the first time possibly know in a trustless manner which fork is correct?

Other Proof of Capacity Advantages

Proof of Capacity is more Decentralized

A benefit of everyday people being able to mine profitably is that the mining power tends to be more decentralized given that it is profitable for everyday people to mine. No longer is mining concentrated in the hands of miners who have spent millions on specialized mining equipment. It could happen that giant data centers will start using their extra free space to mine, but nevertheless, as long as average customers still are able to be profitable by mining, this will not prevent them from mining. Additionally, those giant data centers will earn

approximately the same ROI as customers. Let's face it, in a Proof of Work system, if you start using even your GPU to mine, but ASICs are 1000s of times more cost efficient, your average user isn't even going to try mining. Because they would never win a block and barely help secure the network or make any money for doing so, so what's the point?

Easier new customer Acquisition method than other Algorithms Being ASIC resistance and given that every day people will be more likely to mine means that they can be easily introduced to the coin. There will always be a 'free' way for people to earn Burst, simply by mining for the network. This is a great way to get new customers to join the network. Once you get customers holding on to small amounts of the coin, they feel some loyalty and are more likely to become longer term users, both buying more of the coin themselves as well as encouraging others to use the coin.

Summary

Proof of Capacity offers the best of both worlds and many compelling advantages over Proof of Work and Proof of Stake. Proof of Capacity should be taken seriously and has the potential to win over more customers and if properly marketed, it can quite possibly even become larger than any Proof of Stake or Proof of Work coin out there due to these inherent advantages.

Proof of Capacity is currently running and has been running since August 11th, 2014 and powering Burst. At the moment Burst is the original and at the moment only coin to use the Proof of Capacity algorithm.