Volume 6, Issue I, Jan 2018
eISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

PROOF OF SPACE: AN INCANDESCENT SOLUTION TO THE PROBLEMS OF CRYPTOCURRENCY

Rahul Purushottam Gaonkar

Master of Science in Computer Science
NYU Tandon School of Engineering,
Brooklyn NY 11201
rpg283@nyu.edu

Abstract: *Cryptocurrency is one of the hottest topics in the world right now. More prominently, Bitcoin has recorded huge amounts of gains in the past few months. Bitcoin is based on the Proof of Work technology which comprises of real time computations of a given puzzle in shortest amount of time to gain a reward. This method utilizes a lot of energy and resources of a computer system to solve the real-time puzzle calculations. Even though this method seems like a lucrative mean of generating rewards, the energy consumption among others, begs the question of affordability both on the environment as well as the wallet. An alternative solution, Proof of Space has been explored in this paper with the use of a test attack to gauge its efficiency. We present a solution for the common 51% attack for a Proof of Space system. 51% attack has higher success rate if there is only one type of storage device used in the system. Our proposed solution is to let mining power be determined by both memory size and memory access time. This added factor of memory access time makes it costlier to acquire enough mining power for a 51% attack to occur, because memory device with less memory access time is much more expensive than memory devices having more access time. Our analysis shows that this difference in the expense i.e. memory access time becomes significant in systems with large number of miners or in systems with a long matching phase to stop the 51% attack.*

Keywords*: fork, blockchain, miners, Proof of Work, Proof of Space, Cryptocurrencies, plots, scoops, generation signature, block height, vote, blockchain trimming.*

1. INTRODUCTION

With the dawn of the modern technology, many experts are claiming a new "Technological Revolution" may well be underway. One such example of this revolution which has rapidly caught on to the trend like wildfire. Unprecedented expansion of the methods and applications of Proof of Work Systems in Cryptocurrencies like Bitcoin has provoked serious questions about the currency's long-term sustainability. These questions, among most, include the skepticism regarding the concerns over the emergence of a powerful mining authority controlled by a handful of powerful entities as well as the volatility in such a product.

Both problems add fuel to the debate that Proof of Work may not be the best system for the handling of Cryptocurrencies. Due to this, researchers believe that the idea of a Proof of Space system would be a more efficient application in the field of Cryptocurrencies as it is not only an environmental friendly but also a decentralized alternative due to the lower energy cost achieved through the reduced number of real time computations [1-2]. This can happen only because the major chunk of computations is performed up-front and stored in the disk. Thus, allowing the system to perform comparisons with these pre-computed values during mining and lower the variance of memory access times between machines respectively. In proof of Space System, the miners can mine on any fork and need not concentrate their mining power on a fork of the block chain as it uses pre-generated values for mining. One of the famous cryptocurrencies which uses the Proof of Space system is Burstcoin. Even if Proof of Space System promises to provide better decentralization as compared to Proof of Work System, a large group of miners can always act like attackers and can try to mine along the wrong blockchain thereby eventually controlling the mining power of the system and hampering its security. The most common example of this type of attack is the 51% attack. In this attack, cryptocurrency network's miners with 51% of the network's mining power using comparatively large storage devices to store the precomputed solutions plan to attack the system by mining along the wrong blockchain. To address this issue of the 51% attack, we have proposed a Proof of Space system in which mining power is not only dependent on the storage capacity of a machine but also the memory access time of the storage device used (i.e. For example, memory access time of SSD is less as compared to that of HDD). This will, in turn, reduce the probability of having a 51% attack in the proof.

2. BACKGROUND

In the traditional Proof of Space System designed for Cryptocurrencies like Burstcoin, the mining power is completely dependent on the amount of storage used to store the computations performed up-front during the initial setup of the system. This system reduced the real-time computation cost as it just simply matches values with the set of pre-computed values stored in the storage space. This system also provides better decentralization as the miners don't have to install any external and expensive ASIC systems as in Proof of Work Systems which drain a lot of resources thus making them difficult to implement on a financial scale as well as an environmental impact scale. This decentralization prevents a single miner to control a large portion of the network's mining power thereby enhancing the security of the system [1-2]. This traditional system of Proof of Space, wherein mining power is completely dependent on the

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS…..

amount of storage space available, is highly vulnerable to a 51% attack. A group of miners that constitute 51% of the network's mining power using comparatively large storage devices to store the up-front performed computations plan to attack the system by mining along the incorrect blockchain which gets accepted to the system thereby dropping legitimate blockchain transactions and hampering the security of the system. In our work, we are trying to devise a Proof of Space system where the mining power is not only dependent on the amount of storage space available but also the memory access time of the storage device used. The significance of variance of memory access time of different storage devices used in different machines(miners) seems to be quite small in performing a 51% attack when considered for small cryptocurrency system with less miners or in cryptocurrency systems where less time is required in the matching phase of the system (i.e. less number of computations). However, the significance of variance of the memory access time can be considerable in the attack which consists of a very large cryptocurrency system with more number of miners or in cryptocurrency systems where a large amount of time is required in the matching phase of the system (i.e. more number of computations) to mine a coin. The probability of 51% attack in such large systems would be less if we consider that the mining power is not only dependent on the amount of storage space available but also the memory access time of the storage device used because to perform an attack, storage devices should satisfy both the properties (i.e. should have large amount of storage space and should have considerably less memory access time) which would make them considerably expensive.

3. THREAT MODEL

The proposed system would be highly vulnerable to the 51 % attack if it is implemented in small cryptocurrency systems with less miners or in cryptocurrency systems where less time is required in the matching phase of the system (i.e. less number of computations) or both to mine a coin.

1. Threat: A small systems with less number of miners. If a system has less number of miners, the significance of variance in memory access time of different storage devices (i.e. SSD, HDD) used in different machines(miners) would be quite small in performing a 51% attack thereby making it highly vulnerable to it.

Risk: It gives the group of attackers complete control of the system's mining power i.e. system's transactions so that they can manipulate them based on their needs.

Solution: One possible solution which is hard to implement is by making the time taken during the matching phase of the system considerably large (i.e. large number of computations) so that the variance of memory access time of different machines(miners) becomes a significant factor to be considered while performing 51% attack which would reduce the probability of 51% attack.

2. Threat: A system where the matching phase time for providing the proof of space is less (i.e. considerably small number of computations). If a system is designed such that the matching phase time for providing the proof of space is considerably less such that the significance of variance in memory access time of different storage devices (i.e. SSD, HDD) used in different machines(miners) would be quite small in performing a 51% attack thereby making it highly vulnerable to it.

Risk: It gives the group of attackers complete control of the system's mining power i.e. system's transactions so that they can manipulate them based on their needs.

Solution: One possible solution to be implemented is by increasing the number of miners in the system i.e. making large systems in such a way that the variance of memory access time of different machines(miners) becomes a significant factor to be considered while performing 51% attack which would reduce the probability of 51% attack.

4. DESIGN

In our proposed system which is based on Proof of Space, miners perform some amount of work up-front and store it in their storage devices i.e. Miners generate and cache chunks of data known as 'plots', and are divided into portions known as 'scoops'[3]. Plot chunk is generated by taking a public address and a nonce. Once this is done, a hash function is run on this output and generates an intermediate output. This intermediate is again hashed and appended to the previous stage output multiple times until all the plot chunks and their contents are populated. Once this is done, the whole plot output is XORed. Plots are staggered together so chunks of the same scoop number are together, then written to disk [3]. Each block has a generation signature(GenSig). This GenSig can only be derived by the previous block's GenSig and its miner, thus making it difficult to manipulate. When actual mining takes place, the most recently computed GenSig, along with the derivative of the BlockHeight, will generate the Target Value. The Block Height corresponds to the number of blocks in the BlockChain computed till most recent GenSig [3]. When mining, the scoop number to be used for a block is derived from the generation signature and the block height, thus allowing the miner to read all the relevant scoops (each plot will have 1 relevant scoop, and staggering allows for larger sequential read with less seeking). However, it must be noted that only a small fraction (~0.5%) of the stored data will be needed to be read by each block[3].The GenSig is hashed with each scoop. 8 bytes are taken from the hash, then divided by a scaling factor (inverse difficulty). The resulting number, the DEADLINE, is a number which corresponds to the number of seconds required for the address/nonce combination to announce a new block after the generation of the previous block. The miner's hardware can just sit idle until this threshold value is reached, or a new block is formed. The address/nonce is included in the block as proof of eligibility, and the block is signed by that address [3].The proposed system will be designed as described above in such a way that the miners with storage devices that have more storage space and require less time to read data (Seek Time + Rotational Latency + Data Transfer Rate) will have more mining power in a network. This design constraint will reduce the probability of a 51% attack in large systems (with many miners or with a large amount of time required during the matching (verification) phase of the Proof or both) as the group of attackers will not only have to consider the amount of storage of the storage device but also will have to consider the time taken to access the data by a storage device while performing the attack. Storage devices that satisfy both these constraints of large storage space and less time to access the data will be considerably expensive

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

thereby discouraging some attackers from performing a 51% attack.

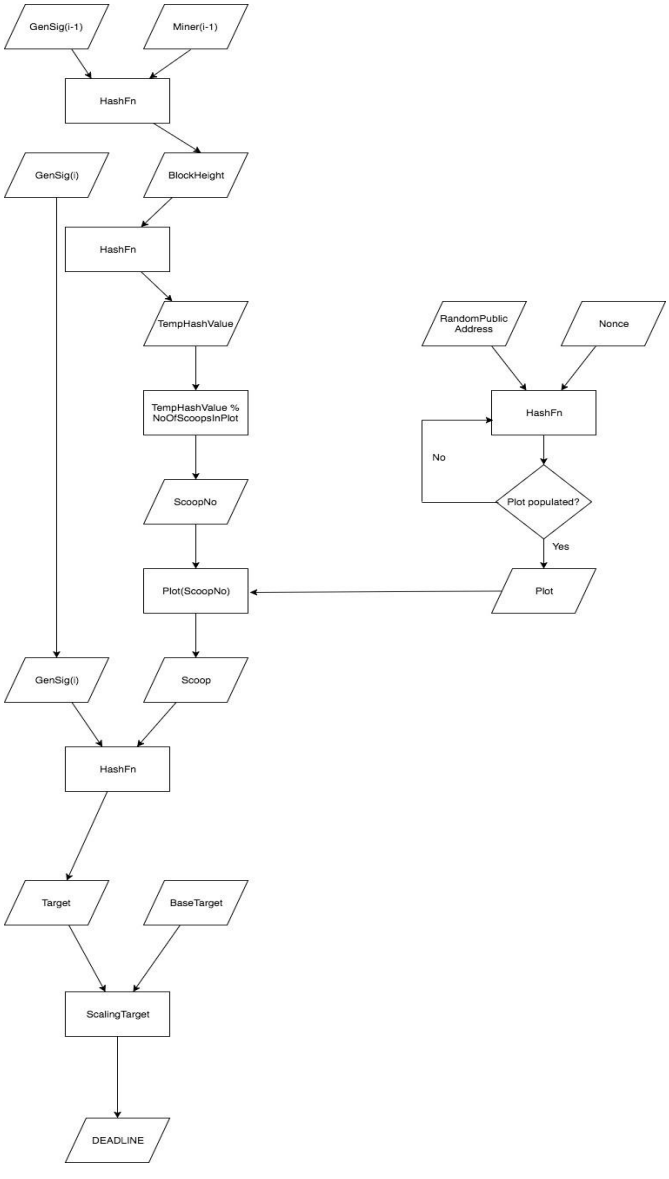

Figure 1: Flowchart of the Process

5. IMPLEMENTATION & EVALUATION

Our proposed system targets the amount of storage and time taken to read the data ((Access Time i.e. Seek time + Rotational Latency) + Data Transfer Rate) of the different types of storage devices used by the miners during the matching phase of the Proof. So, the miner with storage devices having large storage space and that require less time to read the data possess more mining power.

As, we can see from the above table that different storage devices have different memory access time, data transfer rate, power consumptions and purchase prices. The storage device with large storage space, less time taken to read the data and less power consumption are comparatively expensive than other memory devices. So, this can discourage group of attackers to perform a 51% attack thereby reducing the probability of 51% attack as their storage devices should not only have large storage space but should also require less time to read a data thereby making the attack expensive. But since the difference in time taken to read the data of different storage devices used by the miners is minimal, the proposed system will reduce the probability of 51% attack only in large system with many miners or in system where the matching phase time of the proof is large enough such that the cumulative difference in time taken to read the data of different storage devices used by the miners is significant.

Table 1: Comparative Study of some set of storage devices based on different criteria [4-7].

Disk Type	HDD	SSD	Flash memory	Mram
Device Name	HGST Hitachi 0F14685 / HUS724020ALE640 2TB 3.5" 6Gbps 7.2K SATA Hard Drive[1]	Intel SSDSC2BA400G3T 400GB SATA SSD[2]	Sandisk CZ48 128GB USB 3.0 Flash memory Drive - SDCZ48-128G-U46[4]	MR4A08 BYS35[3]
Access Time	8 ms	50 µs read/ 65 µs write	Up to 100 MBps	Max 35 ns
Data Transfer Rate	Interface transfer rate = 600 Mbps max. Sustained rate = 181 Mbps	500 Mbps read 460 Mbps write (sequential)		Data bus width = 8 bit
Power Consumption (Read/Write)	11.4 (W)	5.4 mW		.65 W
Power Consumption (Startup current)	2.0 (+12V)			
Power Consumption (Unloading Idle State)	5.7 (W)			
Power Consumption (idle state)	6.9 (W)	650 mW		
memory	2TB	400GB	128GB	16 Mbit = 2 MB
Price for unit ($)	69.5	395	26	33.63

Test Case: Consider 'n' miners in a system such that all of them have the same storage space say 500GB.So in traditional Proof of Space system, 51% of the 'n' miners possess 51% mining power and can perform the 51% of the 'n' miners possess 51% mining power and can perform the 51% attack. But, if we consider that 51% of the 'n' miners have HDD as their storage device and the rest 49% have SSD then for some large value of 'n' our proposed system can prevent the 51% attack as the cumulative difference in the time taken to read the data (access time + data transfer rate) would be significant.

6. RELATED SOLUTIONS

1. Distribution of free tickets/votes: Miners are given free tickets/votes instead of block rewards and the miners get

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS…..

their block reward by casting their single vote on the right chain in future. Also, every time when a block is mined by the miner himself then the miner should include atleast one vote of another miner or he will be punished. After a particular time interval, the miner gets not only the block reward of the block they mined but also a part of block reward of another miner who include their votes. These votes strengthen the blockchain as votes once given cannot be removed or moved to other blockchain and the miners also cannot vote on multiple chains. Using this method can prevent cheating, if a miner catches a cheater who is not following the above rules and includes that cheat in his block. The miner who includes this cheat in his block also gets to keep the cheater's block reward[8].

2. Distribution of free tickets/votes and their usage depending on a specific time interval: Miners are given free tickets/votes and they get their block reward by casting their votes on the same right fork in between the assigned time interval. For Example, if a miner is given 3 votes, he can cast the first vote only between blocks 100 to 200, can cast the second vote only between blocks 200 to 300 and the third vote only between blocks 300 to 400.This distribution of casting votes will further strengthen the blockchain. Also, every time when a block is mined by the miner himself then the miner should include atleast one vote of another miner that too within the right number of blocks or he will be punished. Using this method can prevent cheating, if a miner catches a cheater who has voted on multiple forks and includes those votes in his block. The miner who includes those votes in his block also gets to keep the cheater's block reward [8].

3. Temporary introduction of Proof of Stake component: We can introduce temporarily proof of stake component in the system. Proof of stake component will basically check for the sum of priorities of the transactions in both the legitimate fork and the fake fork and accept the fork with a greater sum value. Priorities of the transactions are higher if they have an old cryptocurrency involved i.e. if the transactions involve burst coins held for a longer period. By using this property, Proof of Stake component will basically ignore the longest fake fork and accept the legitimate fork as attackers will quickly run out of old, high priority cryptocurrencies in the process of 51% attacking the system. This method will just reduce the probability of the disruption of the system through 51% attack but cannot completely stop 51% attack as a group of miners attacking the system will have a lot of high priority cryptocurrencies with them. But this solution is a temporary fix to control the damage limitation in case of an emergency to prevent shutting down of the system by a 51% attack. The proof of Space system introducing this Proof of Stake component can ignore the Proof of Stake component during the Blockchain trimming phase [8].

7. CONCLUSION

Proof of Space is an emerging idea that may prove superior to Proof of Work with its many advantages such as decentralized system and low power consumption. However, there are still threats to Proof of Space that can be detrimental, such as the 51% attack. Thus, we explore a potential solution that can help minimize the chance of a 51% attack occurring. The improved Proof of Space system shall have mining power that is dependent on both the storage capacity and memory access time of the storage device used. This will significantly increase the expense of a 51% attack, because memory devices with less memory access time is more expensive (For e.g. SSD is much more expensive than HDD for same amount of memory). The increase expense will increase the difficulty of 51% attacks. However, this solution only helps lower the chance of 51% and it only makes a significant difference in a system with large number of miners or with a long matching phase time, so it is a threat if either of the two scenarios are not present.

REFERENCES

[1] Sunoo Park, Albert Kwon, Joel Alwen, Georg Fuchsbauer, Peter Gazi, Krzysztof Pietrzak. "SpaceMint: A Cryptocurrency Based on Proofs of Space". 2015. https://eprint.iacr.org/2015/528.pdf. (accessed December 2, 2017)

[2] Wikipedia article gives detailed explanation of Proof of Space concept and gives introduction to some of technologies like BurstCoin which has emerged based on this Concept. November 9, 2017. https://en.wikipedia.org/wiki/Proof-of-Space. (accessed December 2, 2017)

[3] Explanation about Proof of Space (Proof of Capacity) on the website of BurstCoin (an application based on this concept) 2017. https://www.burst-coin.org/proof-of-capacity. (accessed December 3, 2017)

[4] DiscTech. "HGST Hitachi 0F14685/ HUS724020ALE640 2TB 3.5' 6Gbps 7.2K SATA Hard Drive.". 2017. www.disctech.com/Hitachi-0F14685-2000GB-SATA-Disk-HDD. (accessed December 2,2017)

[5] DiscTech. "Intel SSDSC2BA400G3T/ SSDSC2BA400G3 6XJ05 400GB 2.5" 6Gbps MLC SED DC S3700 Series SATA SSD".2017. www.disctech.com/Intel-SSDSC2BA400G3T-400GB-SATA-SSD-Drive. (accessed December 2, 2017)

[6] Arrow.com. "MR4A08BYS35 By Everspin Technologies | MRAM".2017. www.arrow.com/en/products/mr4a08bys35/ everspin-technologies. (accessed December 2,2017)

[7] Amazon.com. "SanDisk CZ48 128GB USB 3.0 Flash Memory Drive - SDCZ48-128G-U46: Computers & Accessories." 2017. www.amazon.com/Sandisk-128GB-Flash-memory Drive/dp/B00P8XQPY4/ ref=zg_bs_3151491_7? _encoding=UTF8& psc=1 EW3AAT. (accessed December 2, 2017)

[8] Matthew Czarnek. An article explaining why Proof of Capacity should be taken seriously. June 16, 2017. https://www.burstcoin.ist/2017/06/16/why-proof-of-capacity-should-be-taken-seriously-2015-reprint-part-1/. (accessed December 5, 2017).