Suacoin: Ecological friendly proof-of-work cryptocurrency

Armando Machado, J. Augusto Domingues
amach@suacoin.com jadom@suacoin.com
www.suacoin.com

Abstract. This fork of earlier version bitcoin provides an automatic difficulty reset when no block is mined for a period of over 24h. With a 21 million supply and it's own blockchain with master nodes distributed across regions around the planet to provide faster transactions. Uses the SHA-256 crypto for hardware compatibility, allowing current holders of SHA-256 compatible mining equipment such as ASIC or GPUs to mine suacoins with lower energy consumption and difficulty. It's protected from difficulty mount attack, by automatic reset built-in. After block 500,000 or another point in time, for sake of the planet fragile ecology, the code and wallets will be updated to use the BLAKE3 crypto instead of SHA-256, giving an incentive for miners to mine before that event.

1. Introduction

Bitcoin [1] and other proof-of-work cryptocurrencies are at present with an astronomical difficulty levels that make it a high energy consumption dependent with an impact on the planet fragile ecosystem [3]. Miners are using high amounts of energy and costly hardware to perform crypto currency mining, so much so, that it's having an impact on the electrical infrastructure of developing countries leading to energy blackouts [4], illegal use of energy by criminal gangs and electricity produce from cool mines being direct to mining instead of serving populations and industry energy needs. Moreover transaction costs have gone through the roof, to the point, it will be extremely costly to send smaller amounts of crypto currency between wallets. So the concept of bitcoin and similar proof-of-work are functional but they are not very efficient.

The Ethereum [2] crypto currency by providing smart contracts and tokens, reduced in part the creation of new altcoins and it's impact on the planet ecology, by fact that these new tokens use a single blockchain: the ethereum blockchain. But ethereum although widely praised, unlike bitcoin, suffers from poor implementation with constant hard-forks [5] to provide bug fixes to previous mistakes and performance.

In recent years, with the advent of proof-of-stake cryptocurrencies it was an attempt to move on from proof-of-work. But the weakness of proof-of-stake is that it doesn't achieve good consensus, unfortunately. People staking their coin can vote for both forks of the blockchain, and can even mine effortlessly in secret. This is not possible with proof-of-work, so they are literally wasting energy by mining both sides of a fork [6].

2. Mining Reward

The initial reward for successful mining is 50 Suacoins and halves every 210,000 blocks. Those mined suacoins will be made available to the miner unconfirmed balance. Only when there is at least another 128 blocks from that original block, will those 50 suacoins become available balance to spend.

The suacoin software uses integer arithmetic (only) and represents 1 Suacoin as 10^8 micro-suacoins. The entitlement of new Suacoins N for a given block height h is:

$$N(h) = 50 * 2^{-\lfloor \frac{h}{210000} \rfloor} + fees$$

Due to implicit rounding-down in integer operations of the C++ language, N(h) drops to 0 for blocks with h >= 34 ∗ 210000. Since the network is calibrated to produce 1 blocks every 10 minutes, this is expected in 34∗210000/(6∗24)/365 ≈ 136 years after Suacoin's start in December 12th, 2018.

Since this is the only source of new Suacoins, their total quantity will never exceed 20999949.9769 ≈ 21 million Suacoins. At the time point of this writing the number of Suacoins in circulation is slightly above 1 million.

The miner receives in addition to new suacoins also the fees of transactions included into the block. The proportion of fees in miner's income varies, currently around 15% and is expected to increase in future.

3. Mining difficulty

The minimum threshold for block validity is hardcoded in the code, such that the expected number of hashes needed to find a solution is 2^{32}. The threshold of validity is regularly re-calibrated by the network such that it takes in average 10 minutes of joint search of all miners of the network to find a valid block. The difficulty of the current search is expressed as a factor of the hardcoded minimum difficulty. The expected work at a difficulty level d is $d * 2^{32}$ hashes.

Mining difficulty is recorded in the block chain in every block. Is calculated as the 73rd byte of the block as a positive number x and 74–75th bytes as a big-endian positive number y. The block chain encoded difficulty is then:

$$d = (2^{16} - 1)\frac{2^{208-8(x-3)}}{y}$$

Difficulty adjustment

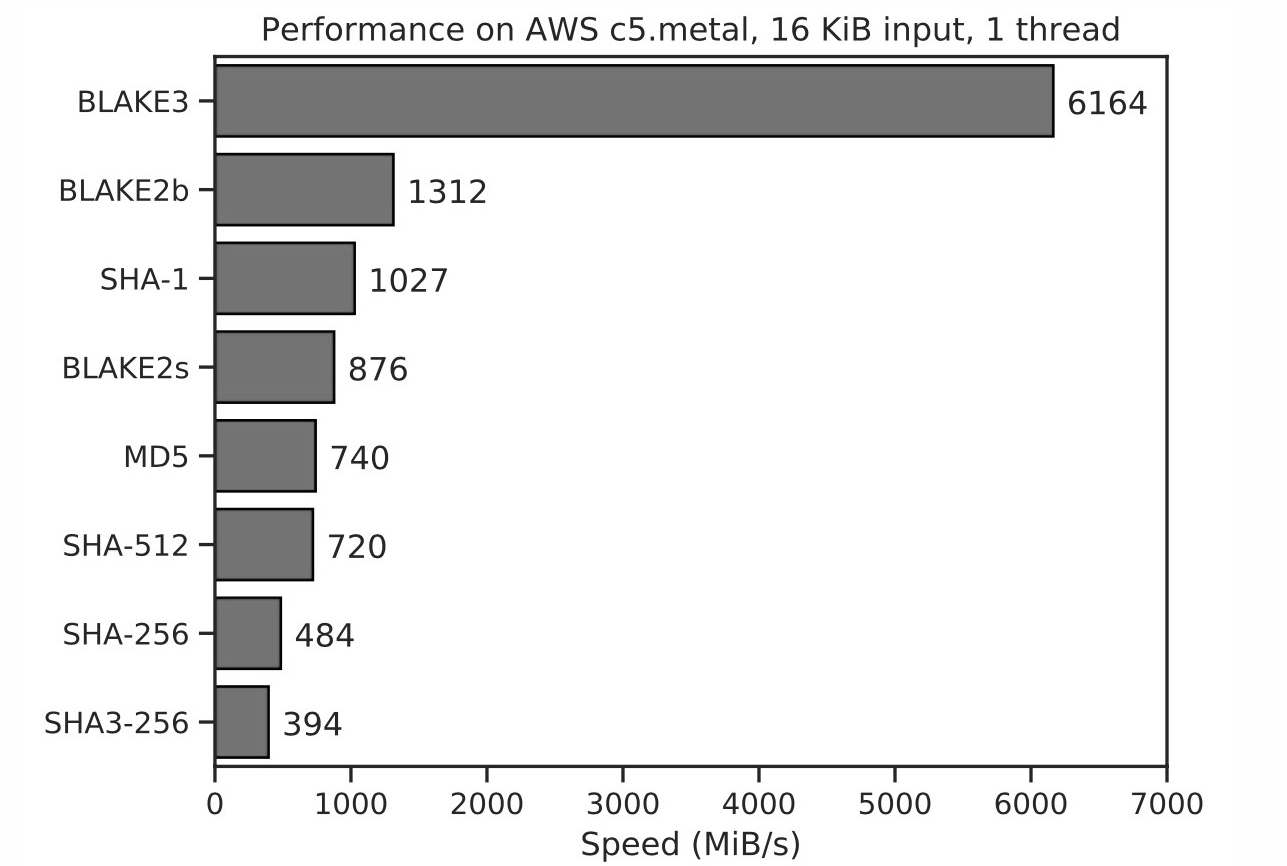
The network re-adjusts mining difficulty such that it can be expected that the network finds a new solution in 10 minutes intervals. The adjustment takes place at every 2016th block. If no new blocked for more than 24 h, the difficulty will be reset to 1. Restarting the difficulty to a level anyone can mine, even with CPU. This way preventing a mining difficulty mount attack by rogue actors.

4. Crypto Swap

After block 500,000 or another point in time in the future, the code and wallets will be updated to use BLAKE3 [7] instead of SHA-256. BLAKE3 is an Extremely Fast and Parallel Cryptographic Hash.

BLAKE3 combines general purpose cryptographic tree hash bao with BLAKE2 in order to provide a big performance improvement over SHA-1, SHA-2, SHA-3, and BLAKE2. It splits its input into 1 KiB chunks and arranges them as the leaves of a binary tree. Each chunk is compressed independently, so the degree of parallelism is equal to the number of chunks.

A benchmark published by the BLAKE3 authors on an Intel Cascade Lake-SP 8275CL processor showing it to be 5x faster than BLAKE2 and 15x faster than SHA3-256.



It must be noted that while BLAKE3 greatly outperforms other hashes such as BLAKE2 and SHA-2/3, it is not the only cryptographic function providing such level of performance.

Security

When it comes to BLAKE3 security, its authors claim it to be 128-bit secure for all security goals, including pre-image, collision, or differentiability attacks. This means BLAKE3 is as secure as SHA3-256 and other hashes that also target 128-bit security.

References

[1] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, “https://bitcoin.org/bitcoin.pdf”, 2009

[2] Vitalik Buterin, "Ethereum Whitepaper", "http://kryptosvet.eu/wp-content/uploads/2021/05/ethereum-whitepaper-kryptosvet.eu_.pdf", 2013

[3] Mason Chock, Mio Shimada, Erik C. Franklin, Camilo Mora, Randi L. Rollins, Katie Taladay, Michael B Kantar, "Bitcoin emissions alone could push global warming above 2°C", “https://www.researchgate.net/publication/328581842_Bitcoin_emissions_alone_could_push_global_warming_above_2C”, 2018

[4] Patrick Sykes and Bloomberg, "Blaming its energy usage, Iran bans crypto mining after widespread blackouts", "https://fortune.com/2021/05/27/iran-ban-crypto-mining-bitcoin-blackout-energy-use/", 2021

[5] Rajeev Kumar, “Ethereum's London Hard Fork upgrade: What's it all about?”, “https://www.moneycontrol.com/news/business/cryptocurrency/ethereums-london-hard-fork-upgrade-whats-it-all-about-7284971.html”, 2021

[6] Abhishek Sharma, "Understanding Proof of Stake through it’s Flaws. Part 2 — ‘Nothing’s at Stake’","https://medium.com/@abhisharm/understanding-proof-of-stake-through-its-flaws-part-2-nothing-s-at-stake-8d12d826956c", 2018

[7] Jack O’Connor, Jean-Philippe Aumasson, Samuel Neves, Zooko Wilcox-O’Hearn, “BLAKE3”, “https://github.com/BLAKE3-team/BLAKE3-specs/blob/master/blake3.pdf”, 2020