README.md

Sugarchain: a PoW blockchain with fast transaction and accurate block reward halving with no rounding errors

Zenny Kim
zennykim.dev@gmail.com

Abstract. Sugarchain is the world's fastest PoW blockchain, that has the first Native SegWit (Bech32) built-in by default. Unlike Bitcoin, Sugarchain has no rounding errors when the block reward is halved. It launched fairly and follows Nakamoto's one-CPU-one-vote.

1. Introduction

Sugarchain is a decentralized, peer-to-peer (P2P) digital currency and payment network supported by an open-source blockchain protocol, launched by Zenny Kim and Volodymyr Biloshytskyi on August 24, 2019 [1]. Through Sugarchain, users can make payments to anyone in the world at the highest speeds ***in 5 seconds***, and the lowest costs compared to other digital assets. For example, the transaction speed of Sugarchain is 120 times faster than Bitcoin, 30 times faster than Litecoin and 12 times faster than Dogecoin.

The Sugarchain Project emerged as an alternative solution to Bitcoin in light of early concerns over Bitcoin's wait times in confirming block transactions and rounding errors in block reward halving. By introducing minor technical modifications to the original Bitcoin source code, Sugarchain allowed for much faster transaction speeds, even lower processing fees and has ***the most accurate block reward halving and total supply*** than any other digital asset, including Bitcoin. Sugarchain also launched following the ***one-CPU-one-vote*** idea proposed by Satoshi Nakamoto himself, thus making YespowerSugar GPU and ASIC resistant. It has also launched as being the first blockchain to have ***Native SegWit (Bech32)*** enabled by default.

As one of the successful derivatives of Bitcoin, Sugarchain is establishing its position as ***the world's fastest PoW blockchain***, complementing and reinforcing Bitcoin in purpose, function, and utility, and challenging our traditional notions of money. The Sugarchain Project has ***never been funded through an ICO or premine***, making it a fair launch. Sugarchain is an entirely community and voluntarily driven project, with no external company or funding supporting it apart from community funding.

** [1]: Bitcointalk: [ANN] Sugarchain [CPU] Launching 2019/08/24 15:00 UTC

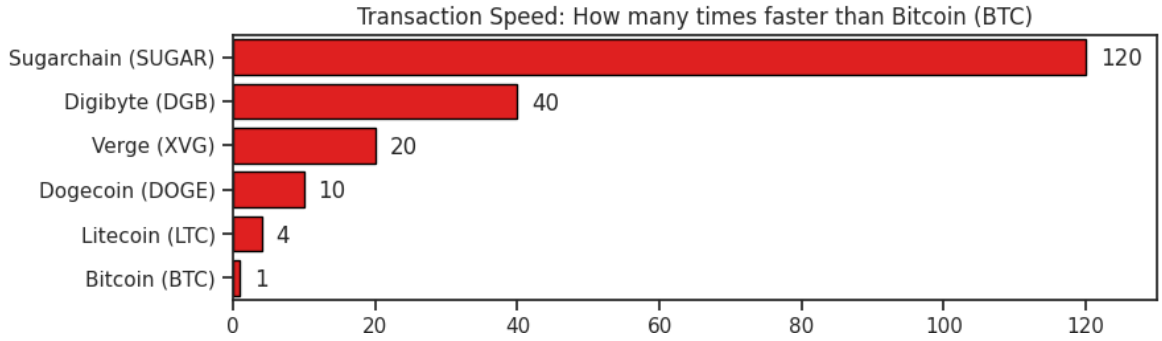
2. Specifications

Block time:	`5` Seconds
Block reward:	`42.94967296` SUGAR
Halving interval:	`12,500,000` Blocks (approx. 2 years)
Total supply:	`1,073,741,824` SUGAR
PoW algorithm:	YespowerSugar (based on Yespower 1.0.1)
Difficulty:	SugarShield-N510 (based on Zcash's modification of Digishield)
Port:	34230 / RPC 34229
Premine:	None: NO ICO, NO Presale, NO Founder's rewards

3. The world's fastest PoW blockchain

- 5 seconds transaction speed [2] :
  - 120x faster than Bitcoin
  - 30x faster than Litecoin
  - 12x faster than Dogecoin

- Transaction speed comparison [3] [4] [5] [6] [7] :



- Don't worry about orphan blocks:
  - According to the testnet results, the average orphan rate is under 3% and no problems occur.

** [2]: Github: SUGAR speed ** [3]: DGB speed ** [4]: XVG speed ** [5]: DOGE speed ** [6]: LTC speed ** [7]: BTC speed

4. Native SegWit (Bech32)

- The first blockchain to have Native SegWit (Bech32) built-in by default.
- Significantly faster and lower cost than legacy transaction.
- Very high probability of detection guaranteed.
- Structure [8] [9] [10]

  - `sugar1qv0ahzfa2ssu47wes89390sl0jz6g05h0267u8g`
    - `sugar`: Human-readable part
    - `1`: Separator "1"
    - `qv0ahzfa2ssu47wes89390sl0jz6g05h0267u8g`: Data part (Base 32 character set encoded):
      - `q`: Witness version
      - `v0ahzfa2ssu47wes89390sl0jz6g05h0`: Witness program
      - `267u8g`: Checksum

** [8]: Github: BIP-173 ** [9]: Youtube: New Address Type for SegWit Addresses by Pieter Wuille ** [10]: File: Keynote Document

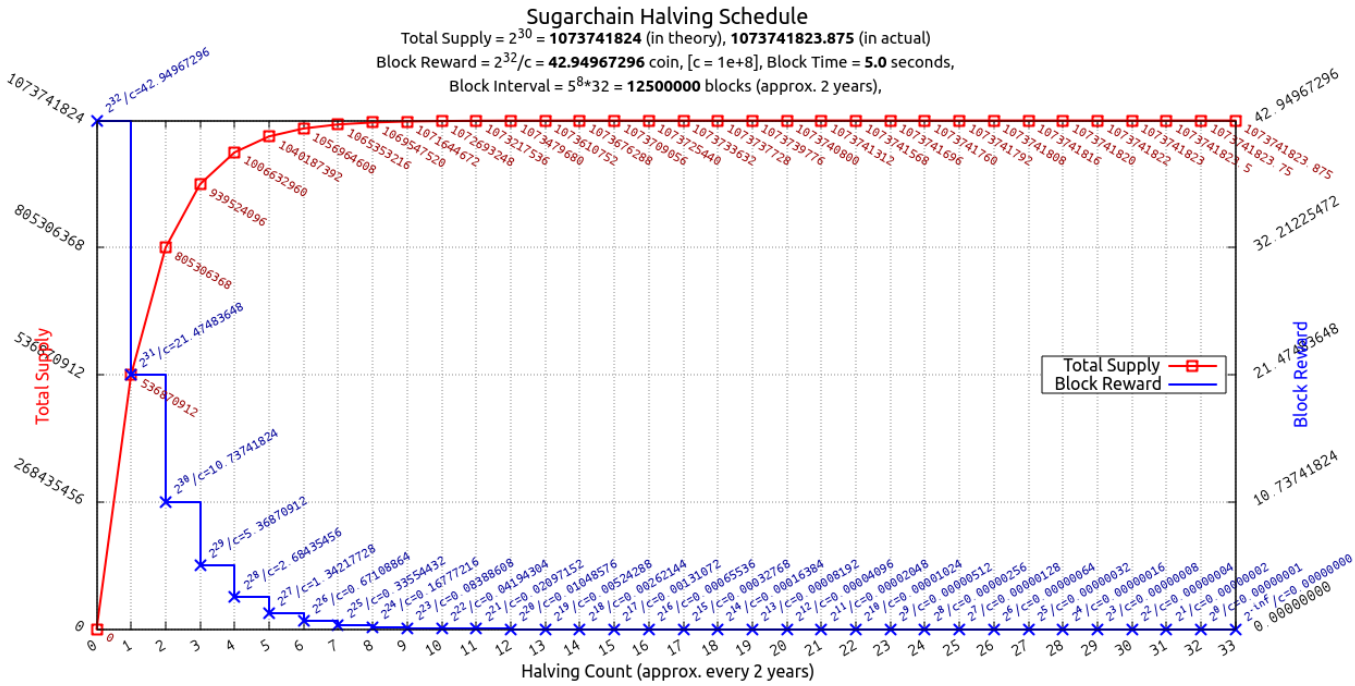
5. Exact halving and total supply

Halving is everything about limiting the total supply. Bitcoin is valuable because its total supply has been strictly limited, unlike traditional currencies. This total supply is controlled only by that halving. There is nothing else. We made this halving better.

$$sugar\ supply\ = \sum_{i=0}^{32} 5^8 \cdot 32 \left[\frac{2^{32}}{2^i} \right]$$

- The formula of Sugarchain's total money supply (in satoshis) [11] [12]
- Block reward:
  - The block reward should be to a ***power of two***, so that it halves correctly.
  - `2^32/1e+8 = 42.94967296 SUGAR` [13]
- Halving schedule:
  - Interval `12500000 blocks (5^8*32)` [14] which is approx. 2 years (62,500,000 seconds).
  - The total number of times halving will occur is 33 times, over the span of approx. 66 years (34,375,000 minutes).
- Total supply:
  - `1073741824 SUGAR` [15] [16] in theory, and `1073741823.875 SUGAR` [17] [18] in actual.
  - The difference is `0.125 SUGAR` . One Satoshi (0.00000001) limitation makes this difference. In addition, this number is meaningful. FYI: `1 GB = 1073741824 Byte (2^30)` .
  - The total supply of Sugarchain is around 51 times greater than Bitcoin.

- Halving chart:



- ▶ Halving table: *(click to expand)*

** [11]: Bitcoin: A Peer-to-Peer Electronic Cash System ** [12]: Bitcoin Wiki: Controlled supply ** [13]: Github: Block Reward ** [14]: Halving Interval ** [15]: Total Supply ** [16]: Total Cap ** [17]: Total Test ** [18]: Total Test(qt)

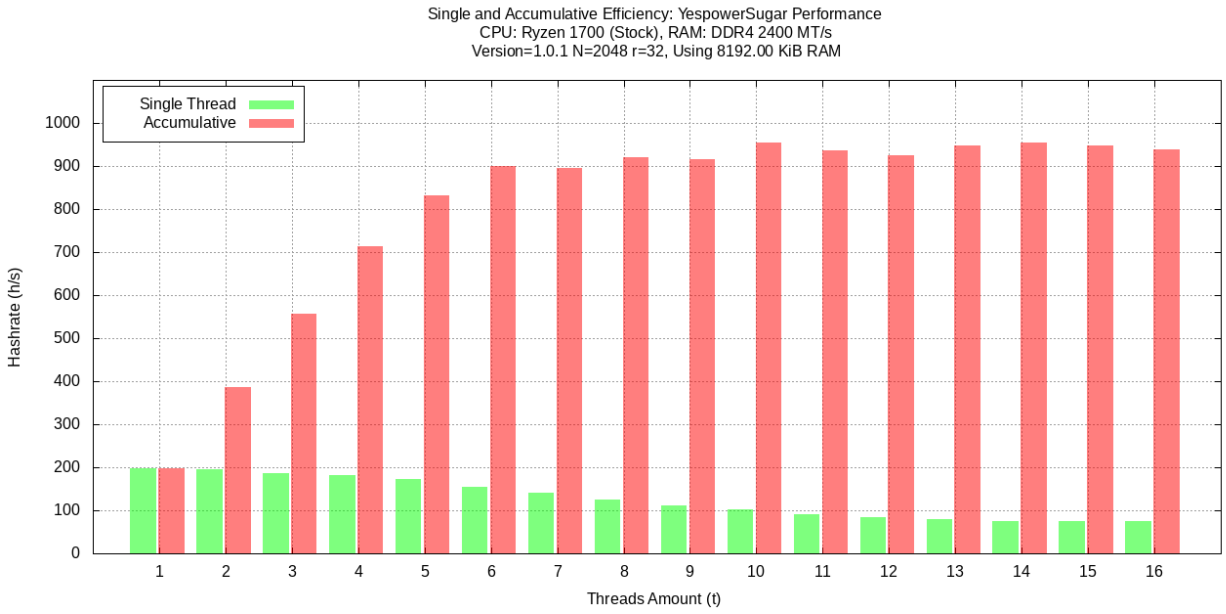
6. one-CPU-one-vote

> “31/Oct/2008 Proof-of-work is essentially one-CPU-one-vote” [11]

Satoshi Nakamoto talked about the importance of decentralized mining in his whitepaper. We want to create a blockchain that anyone can do mining easily without any entry barriers.

- CPU mining only
  - YespowerSugar [19] (based on Yespower 1.0.1) is only for Sugarchain, not compatible with other Yespower coins.
  - The minimum difficulty (powlimit) is set low enough for two reasons. The first is to handle fast block time; The second is to allow mining on slow CPUs.
- Mining efficiency [20] :
  - According to the test results, the most efficient is using ***half of threads*** on a single CPU.
  - YespowerSugar is more suitable for older CPUs, because it is essentially a ***multi-threading resistor***. Suitable for smartphones and Raspberry Pi.

- Benchmark



- NO GPU: GPU mining is not possible.
- NO ASIC: ASIC mining is not possible.

** [19]: Github: YespowerSugar ** [20]: Openwall: yespower - proof-of-work (PoW) scheme

7. Difficulty Adjustment Algorithm (DAA)

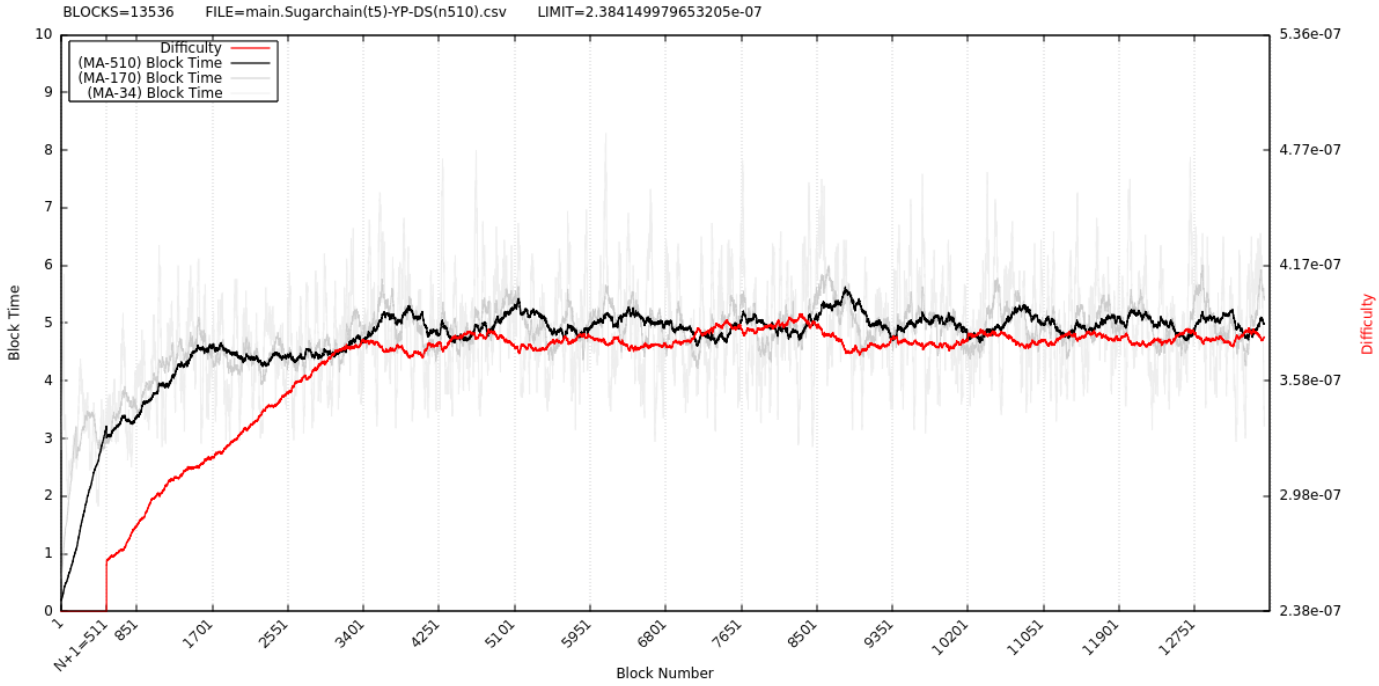
SugarShield-N510 is based on Zcash's modification of Digishield. Unlike the Zcash's modification version, we use a moving average of `510 blocks (approx. 42.5 minutes)` [21] [22]. To keep the block time 5 seconds, SugarShield-N510 adjusts the difficulty level.

- The formula of SugarShield-N510 [23]

```
t = timestamp, h = height,
T = 5 (target block time in seconds),
N = 510 (window size in blocks)
```

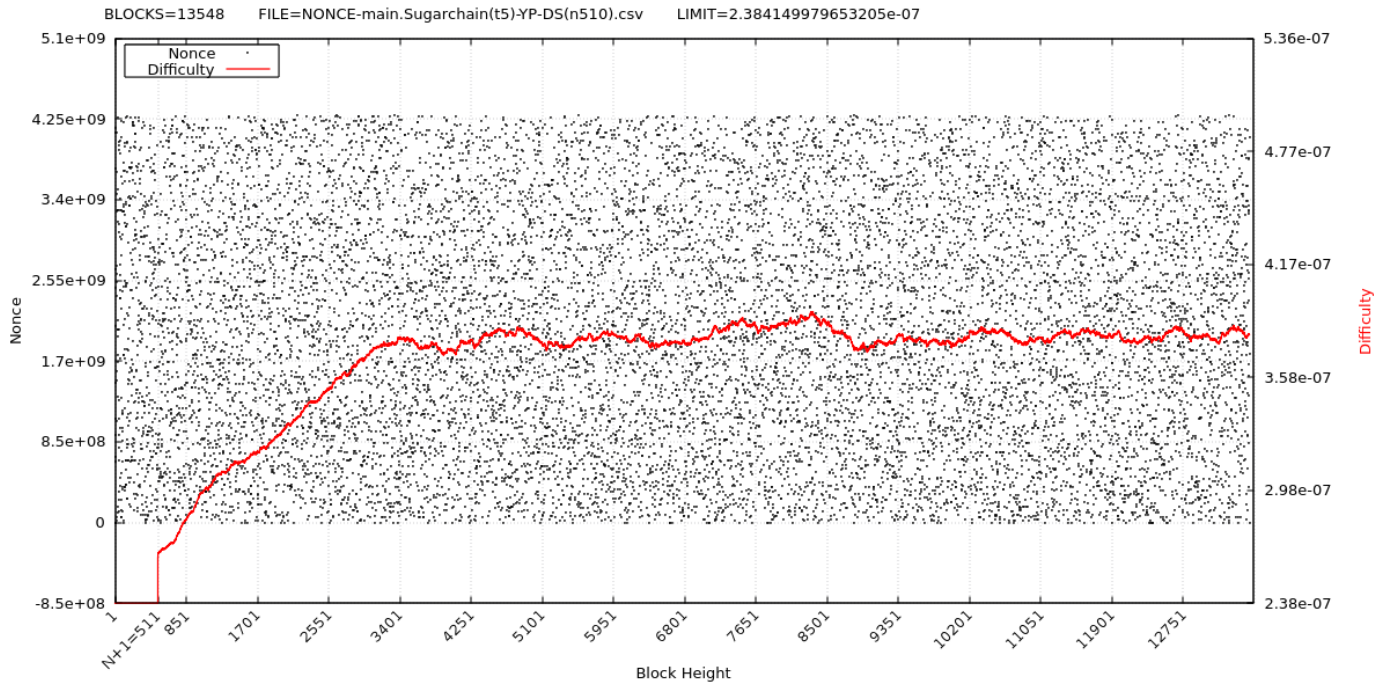
$$target_{h+1} = avg\_N\_targets \cdot (1 + \frac{t_N - t_0}{4 \cdot TN} - \frac{1}{4})$$

- Block time vs difficulty at first launching on testnet



  - It counts from block 1, an adjustment is made at block 511, and the actual control begins at block 512. (log: time-diff)

- Nonce distribution at first launching on testnet



  - The nonce is randomly well distributed. Difficulty changes but no bias. (log: nonce-diff)

** [21]: Github: SugarShield-N510 ** [22]: SugarShield-N510(pow) ** [23]: Summary of Difficulty Algorithms

8. FAQ

- Disk space requirements:
  - Blockchain size growth is around `10 MB per day` and around 3.65 GB per year.
- Network rules:
  - To prevent fraud and timestamp attacks, nodes should be within `70 seconds` [24] of accurate internet time, or they will be banned.
- Selfish mining & time warp attack:
  - Fraud techniques for manipulating timestamps are already known. We use a future time limit (FTL) to prevent this. Blocks that differ `60 seconds` [25] or more from the current head will be banned. (credit: zawy12)

- Header indexing:
  - Using sha256d in header indexing, the initial synchronization speed is as fast as Litecoin.

** [24]: Github: timedata.h ** [25]: Future Time Limit

Links

- Website: https://sugarchain.org
- Github: https://github.com/sugarchain-project
- Explorer: https://1explorer.sugarchain.org
- Explorer(2): https://sugar.wtf
- Explorer(3): https://sugar.wtf/esplora
- Telegram: https://t.me/sugarchain
- Twitter: https://twitter.com/sugarchain_dev
- Bitcointalk: https://bitcointalk.org/index.php?topic=5177722.0