<h1 align="center">
Sugarchain: a PoW blockchain with fast transaction and accurate block reward halving with no rounding errors
</h1>

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.

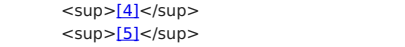
As one of the successful derivatives of Bitcoin, Sugarchain is establishing its position as ***the world's fastest PoW blockchain***, complementing and reinforcing Bitcoin in purpose, function, and utility, and challenging our traditional notions of money. The Sugarchain Project has ***never been funded 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.

<small>** [1]: Bitcointalk: [ANN] Sugarchain [CPU] Launching 2019/08/24 15:00 UTC (https://bitcointalk.org/index.php?topic=5177722.0)
</small>

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.

<small>** [2]: Github: SUGAR speed (https://github.com/sugarchain-project/sugarchain/blob/d2d13cacd9e7c2640a02e6392978a26df06f9eb8/src/chainparams.cpp#L187)
** [3]: DGB speed (https://github.com/digibyte/digibyte/blob/82414be2e78bd136daeb91f55c72768a9b700957/src/chainparams.cpp#L88)
** [4]: XVG speed (https://github.com/vergecurrency/verge/blob/4ae658a47ff3ea7af269cf408387e8265cccf197/src/chainparams.cpp#L85)
** [5]: DOGE speed (https://github.com/dogecoin/dogecoin/blob/0b46a40ed125d7bf4b5a485b91350bc8bdc48fc8/src/chainparams.cpp#L89)
** [6]: LTC speed (https://github.com/litecoin-project/litecoin/blob/81c4f2d80fbd33d127ff9b31bf588e4925599d79/src/chainparams.cpp#L74)
** [7]: BTC speed (https://github.com/bitcoin/bitcoin/blob/48c1083632687a42ac603d4f241e70616a1d3815/src/chainparams.cpp#L77)
</small>

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]

  <img src="image/bech32_structure.png" width="75%">

<small>** [8]: Github: BIP-173 (https://github.com/bitcoin/bips/blob/master/bip-0173.mediawiki)
** [9]: Youtube: New Address Type for SegWit Addresses by Pieter Wuille (https://www.youtube.com/watch?v=NqiN9VFE4CU)
** [10]: File: Keynote Document (https://prezi.com/gwnjkqjqjjbz/bech32-a-base32-address-format/)
</small>

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.

- The formula of Sugarchain's total money supply (in satoshis)
  ^[11]
  ^[12]
  <img src="image/supply_formula.png" width="40%">

- 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]

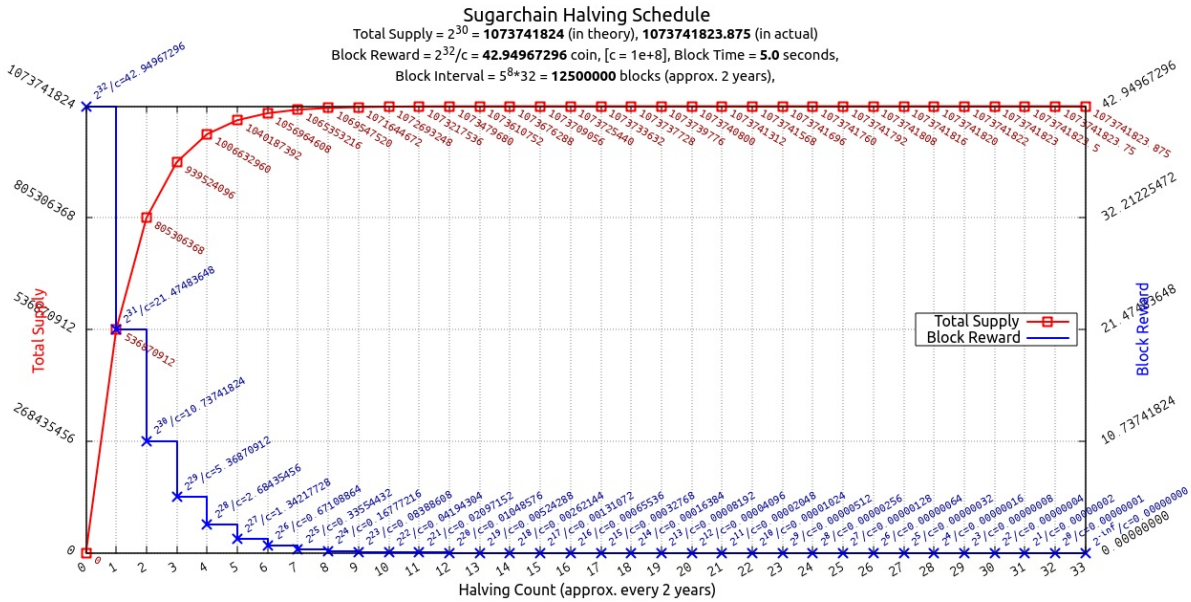
- Halving schedule:

  - 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:



<!-- BEGIN - Hidden Halving table: -->

- <details><summary>Halving table: (click to expand)</summary>

Sugarchain Halving Schedule

Yumekawa v0.16.3 – 20190424

Date	Count	Supply	Pow	Reward	Virtual
2019	0	0	2^{32}	42.94967296	
2021	1	536870912	2^{31}	21.47483648	
2023	2	805306368	2^{30}	10.73741824	
2025	3	939524096	2^{29}	5.36870912	
2027	4	1006632960	2^{28}	2.68435456	
2029	5	1040187392	2^{27}	1.34217728	
2031	6	1056964608	2^{26}	0.67108864	
2033	7	1065353216	2^{25}	0.33554432	

2035	8	1069547520	2^{24}	0.16777216	
2037	9	1071644672	2^{23}	0.08388608	
2039	10	1072693248	2^{22}	0.04194304	
2041	11	1073217536	2^{21}	0.02097152	
2043	12	1073479680	2^{20}	0.01048576	
2045	13	1073610752	2^{19}	0.00524288	
2047	14	1073676288	2^{18}	0.00262144	
2049	15	1073709056	2^{17}	0.00131072	
2051	16	1073725440	2^{16}	0.00065536	None
2053	17	1073733632	2^{15}	0.00032768	
2055	18	1073737728	2^{14}	0.00016384	
2057	19	1073739776	2^{13}	0.00008192	
2059	20	1073740800	2^{12}	0.00004096	
2061	21	1073741312	2^{11}	0.00002048	
2063	22	1073741568	2^{10}	0.00001024	
2065	23	1073741696	2^{9}	0.00000512	
2067	24	1073741760	2^{8}	0.00000256	
2069	25	1073741792	2^{7}	0.00000128	
2071	26	1073741808	2^{6}	0.00000064	
2073	27	1073741816	2^{5}	0.00000032	
2075	28	1073741820	2^{4}	0.00000016	
2077	29	1073741822	2^{3}	0.00000008	
2079	30	1073741823	2^{2}	0.00000004	
2081	31	1073741823.5	2^{1}	0.00000002	
2083	32	1073741823.75	2^{0}	0.00000001	
2085	33	**(Actual Total Supply) 1073741823.875**	2^{-1}	0	5.00000000E-09
2087	34	1073741823.9375	2^{-2}		2.50000000E-09
2089	35	1073741823.96875	2^{-3}		1.25000000E-09
2091	36	1073741823.984375	2^{-4}		6.25000000E-10
2093	37	1073741823.9921875	2^{-5}		3.12500000E-10
2095	38	1073741823.99609375	2^{-6}		1.56250000E-10
2097	39	1073741823.998046875	2^{-7}		7.81250000E-11
2099	40	1073741823.9990234375	2^{-8}		3.90625000E-11
2101	41	1073741823.99951171875	2^{-9}		1.95312500E-11
2103	42	1073741823.999755859375	2^{-10}		9.76562500E-12
2105	43	1073741823.9998779296875	2^{-11}		4.88281250E-12
2107	44	1073741823.99993896484375	2^{-12}		2.44140625E-12
2109	45	1073741823.999969482421875	2^{-13}		1.22070313E-12
2111	46	1073741823.9999847412109375	2^{-14}		6.10351563E-13
2113	47	1073741823.99999237060546875	2^{-15}		3.05175781E-13
2115	48	1073741823.999996185302734375	2^{-16}	Zero Satoshi Limitation	1.52587891E-13
2117	49	1073741823.9999980926513671875	2^{-17}		7.62939453E-14
2119	50	1073741823.99999904632568359375	2^{-18}		3.81469727E-14
2121	51	1073741823.999999523162841796875	2^{-19}		1.90734863E-14
2123	52	1073741823.9999997615814208984375	2^{-20}		9.53674316E-15
2125	53	1073741823.99999988079071044921875	2^{-21}		4.76837158E-15
2127	54	1073741823.999999940395355224609375	2^{-22}		2.38418579E-15
2129	55	1073741823.9999999701976776123046875	2^{-23}		1.19209290E-15
2131	56	1073741823.99999998509883880615234375	2^{-24}		5.96046448E-16
2133	57	1073741823.999999992549419403076171875	2^{-25}		2.98023224E-16
2135	58	1073741823.9999999962747097015380859375	2^{-26}		1.49011612E-16
2137	59	1073741823.99999999813735485076904296875	2^{-27}		7.45058060E-17
2139	60	1073741823.999999999068677425384521484375	2^{-28}		3.72529030E-17
2141	61	1073741823.9999999995343387126922607421875	2^{-29}		1.86264515E-17
2143	62	1073741823.99999999976716935634613037109375	2^{-30}		9.31322575E-18
2145	63	1073741823.999999999883584678173065185546875	2^{-31}		4.65661287E-18
~	~	~	~	~	~
inf	inf	**(Theoretical Total Supply) 1073741824.0**	2^{32-inf}	Total Supply Reached	0.00E-inf

</details>
<!-- END - Hidden Halving table: -->

<small>** [11]: Bitcoin: A Peer-to-Peer Electronic Cash System (https://bitcoin.org/bitcoin.pdf)
** [12]: Bitcoin Wiki: Controlled supply (https://en.bitcoin.it/wiki/Controlled_supply)
** [13]: Github: Block Reward (https://github.com/sugarchain-project/sugarchain/blob/d2d13cacd9e7c2640a02e6392978a26df06f9eb8/src/validation.cpp#L1155)
** [14]: Halving Interval (https://github.com/sugarchain-project/sugarchain/blob/d2d13cacd9e7c2640a02e6392978a26df06f9eb8/src/chainparams.cpp#L135)
** [15]: Total Supply (https://github.com/sugarchain-project/sugarchain/blob/d2d13cacd9e7c2640a02e6392978a26df06f9eb8/src/validation.cpp#L1147-L1216)
** [16]: Total Cap (https://github.com/sugarchain-

project/sugarchain/blob/d2d13cacd9e7c2640a02e6392978a26df06f9eb8/src/amount.h#L33)
** [17]: Total Test (https://github.com/sugarchain-project/sugarchain/blob/d2d13cacd9e7c2640a02e6392978a26df06f9eb8/src/test/main_tests.cpp#L48-L67)
** [18]: Total Test(qt) (https://github.com/sugarchain-project/sugarchain/blob/d2d13cacd9e7c2640a02e6392978a26df06f9eb8/src/qt/test/paymentrequestdata.h#L437-L468)
</small>

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
  <img src="image/yps_efficiency.png" width="90%">
- NO GPU: GPU mining is not possible.
- NO ASIC: ASIC mining is not possible.

<small>** [19]: Github: YespowerSugar (https://github.com/sugarchain-project/sugarchain/blob/d2d13cacd9e7c2640a02e6392978a26df06f9eb8/src/primitives/block.cpp#L30-L70)
** [20]: Openwall: yespower - proof-of-work (PoW) scheme (https://www.openwall.com/yespower/)
</small>

7. Difficulty Adjustment Algorithm (DAA)

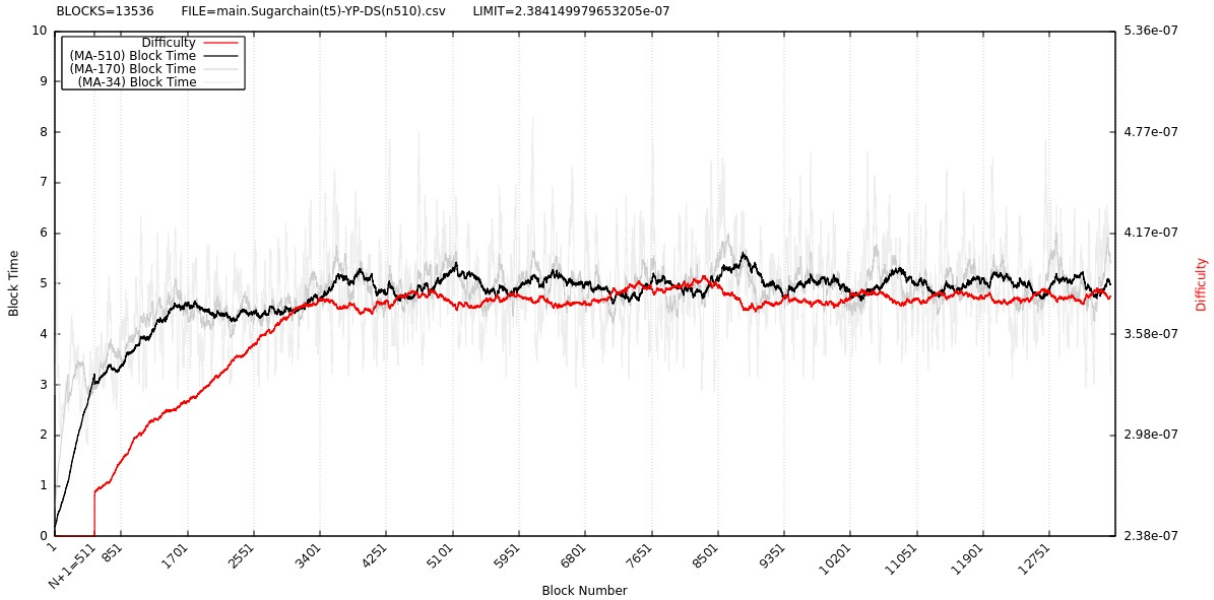
SugarShield-N510 is based on Zcash's modification of Digishield. Unlike the Zcash’s modification version, we use a moving average of `510 blocks (approx. 42.5 minutes)` ^[21] ^[22]. To keep the block time 5 seconds, SugarShield-N510 adjusts the difficulty level.

- The formula of SugarShield-N510 ^[23]

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

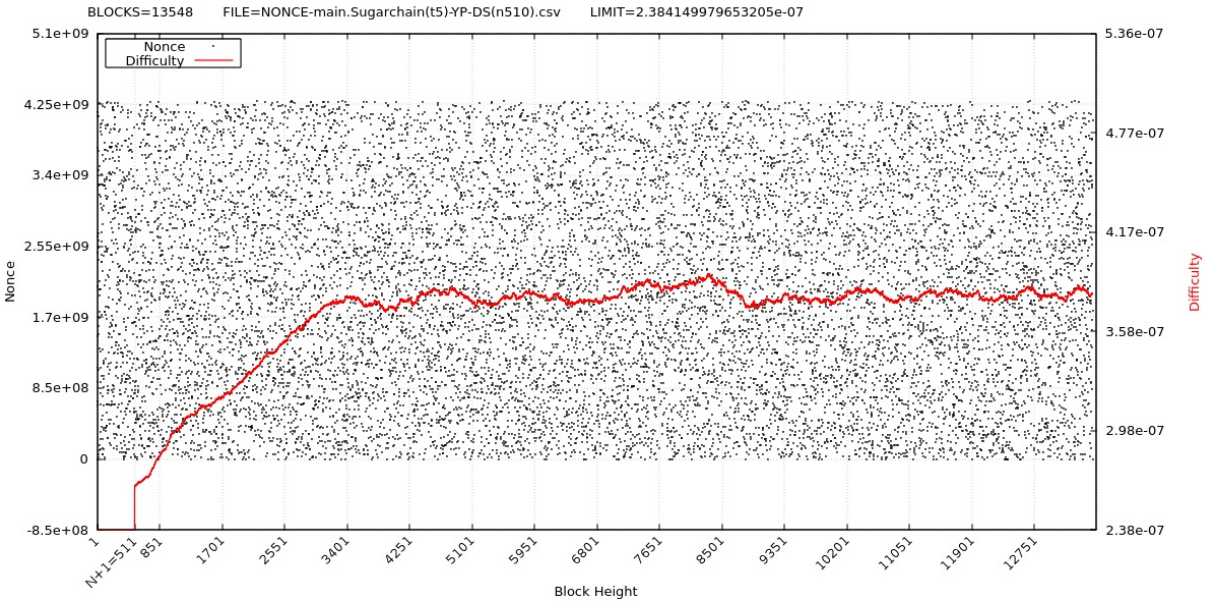
  <img src="image/sugarshield_formula.png" width="50%">

- 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) (https://raw.githubusercontent.com/sugarchain-project/sugarchain-project.github.io/master/log/time_vs_difficulty-13536.log)

- Nonce distribution at first launching on testnet



  - The nonce is randomly well distributed. Difficulty changes but no bias. (log: nonce-diff) (https://raw.githubusercontent.com/sugarchain-project/sugarchain-project.github.io/master/log/nonce_vs_difficulty-13548.log)

<small>** [21]: Github: SugarShield-N510 (https://github.com/sugarchain-project/sugarchain/blob/d2d13cacd9e7c2640a02e6392978a26df06f9eb8/src/chainparams.cpp#L143-L170)
** [22]: SugarShield-N510(pow) (https://github.com/sugarchain-project/sugarchain/blob/d2d13cacd9e7c2640a02e6392978a26df06f9eb8/src/pow.cpp)
** [23]: Summary of Difficulty Algorithms (https://github.com/zawy12/difficulty-algorithms/issues/50)
</small>

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.

<small>** [24]: Github: timedata.h (https://github.com/sugarchain-project/sugarchain/blob/d2d13cacd9e7c2640a02e6392978a26df06f9eb8/src/timedata.h#L23)
** [25]: Future Time Limit (https://github.com/sugarchain-project/sugarchain/blob/d2d13cacd9e7c2640a02e6392978a26df06f9eb8/src/chain.h#L36)
</small>

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