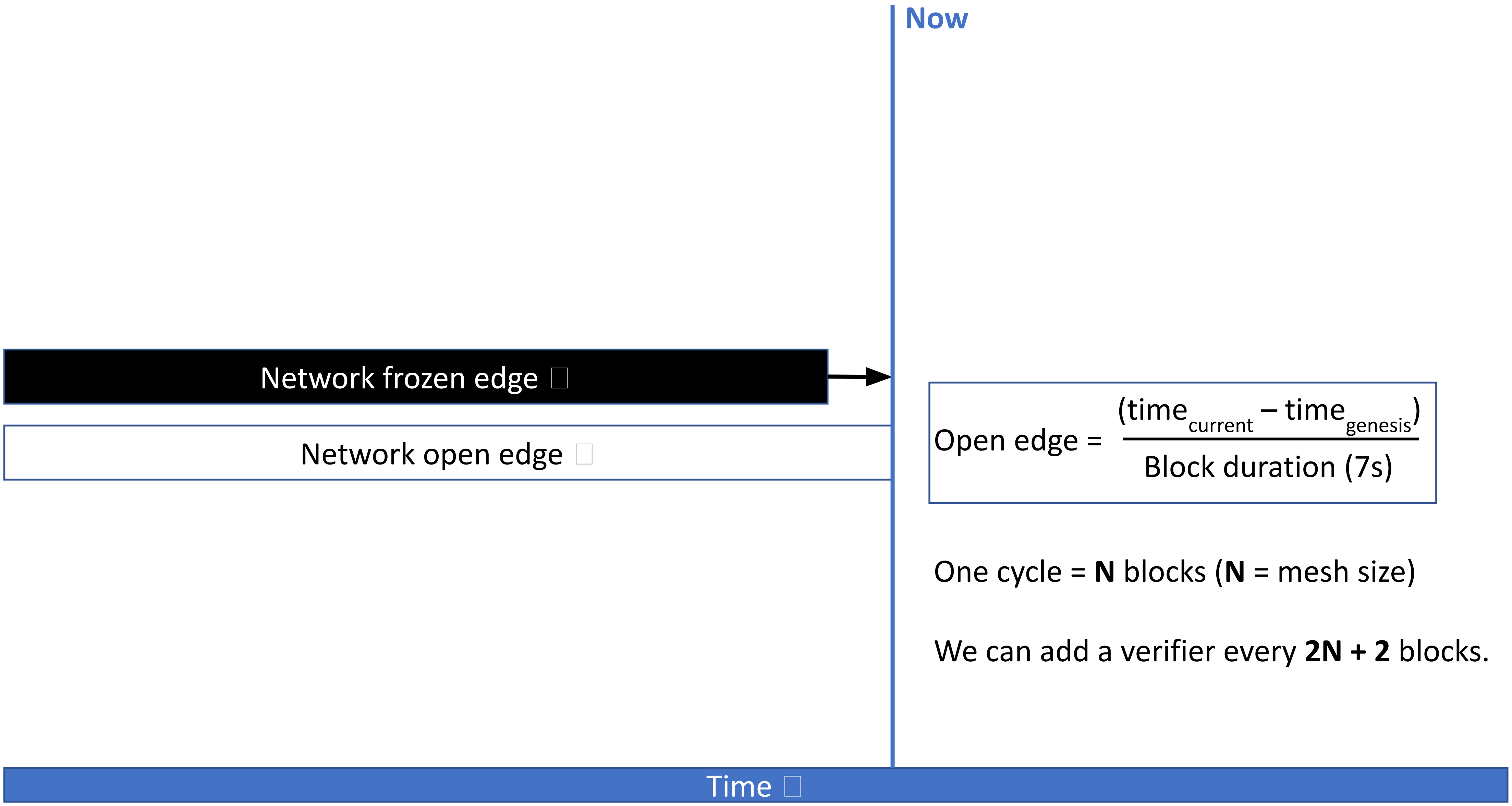
Nyzo design document v0.3

@jimtalksdata

Design goal

- Advance the frozen edge as fast as possible…
- But no further than the open edge
- We need at least 50% of verifiers to agree on the consensus to freeze an edge



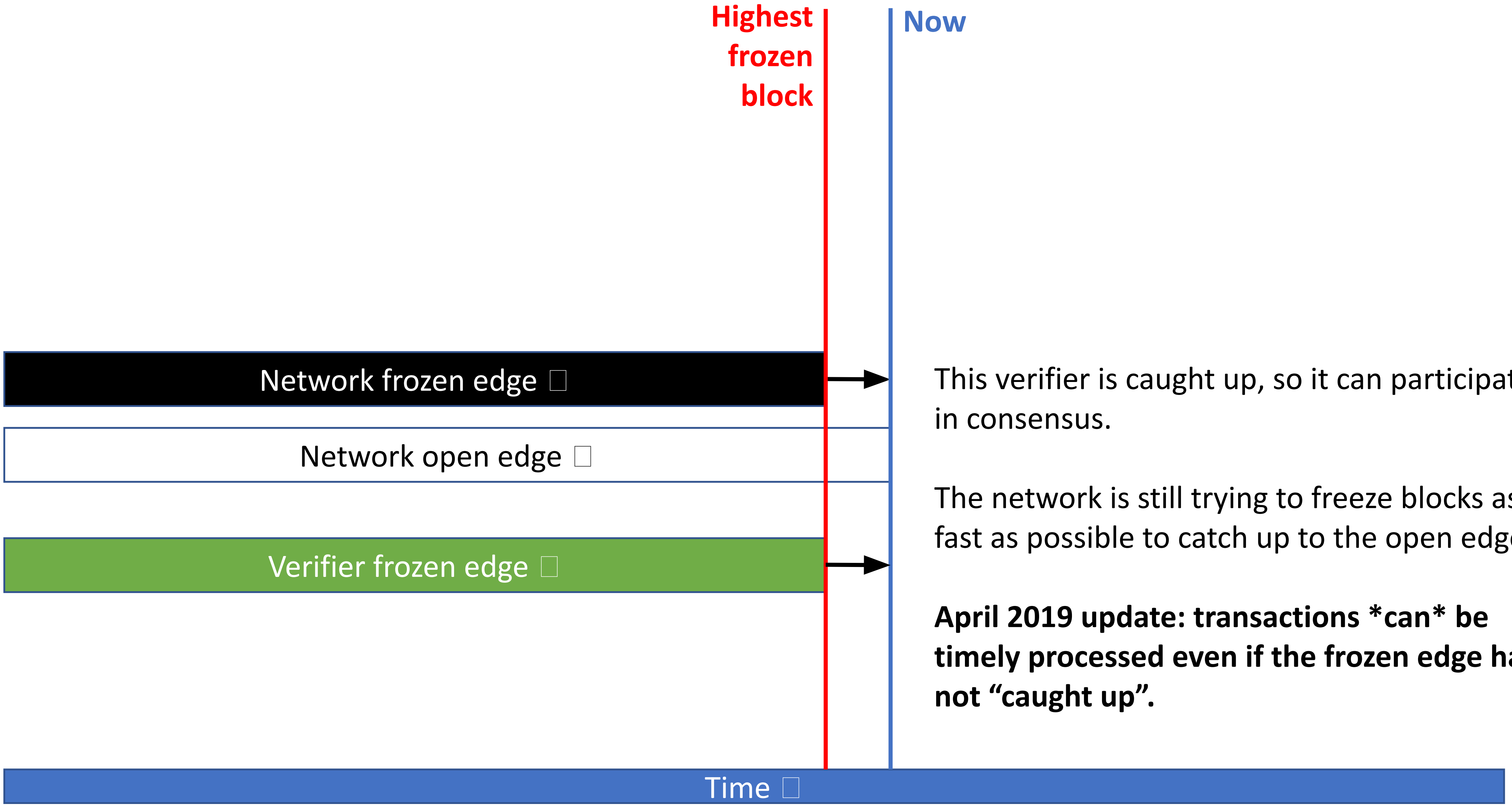
$$\text{Open edge} = \frac{(\text{time}_{\text{current}} - \text{time}_{\text{genesis}})}{\text{Block duration (7s)}}$$

One cycle = **N** blocks (**N** = mesh size)

We can add a verifier every **2N + 2** blocks.

Network and verifier

- Verifiers acquire blocks as fast as possible to match the network's **frozen edge**
- When the frozen edge is caught up, verifiers can vote for the next **block hash**



Highest frozen block

Now

Network frozen edge □

Network open edge □

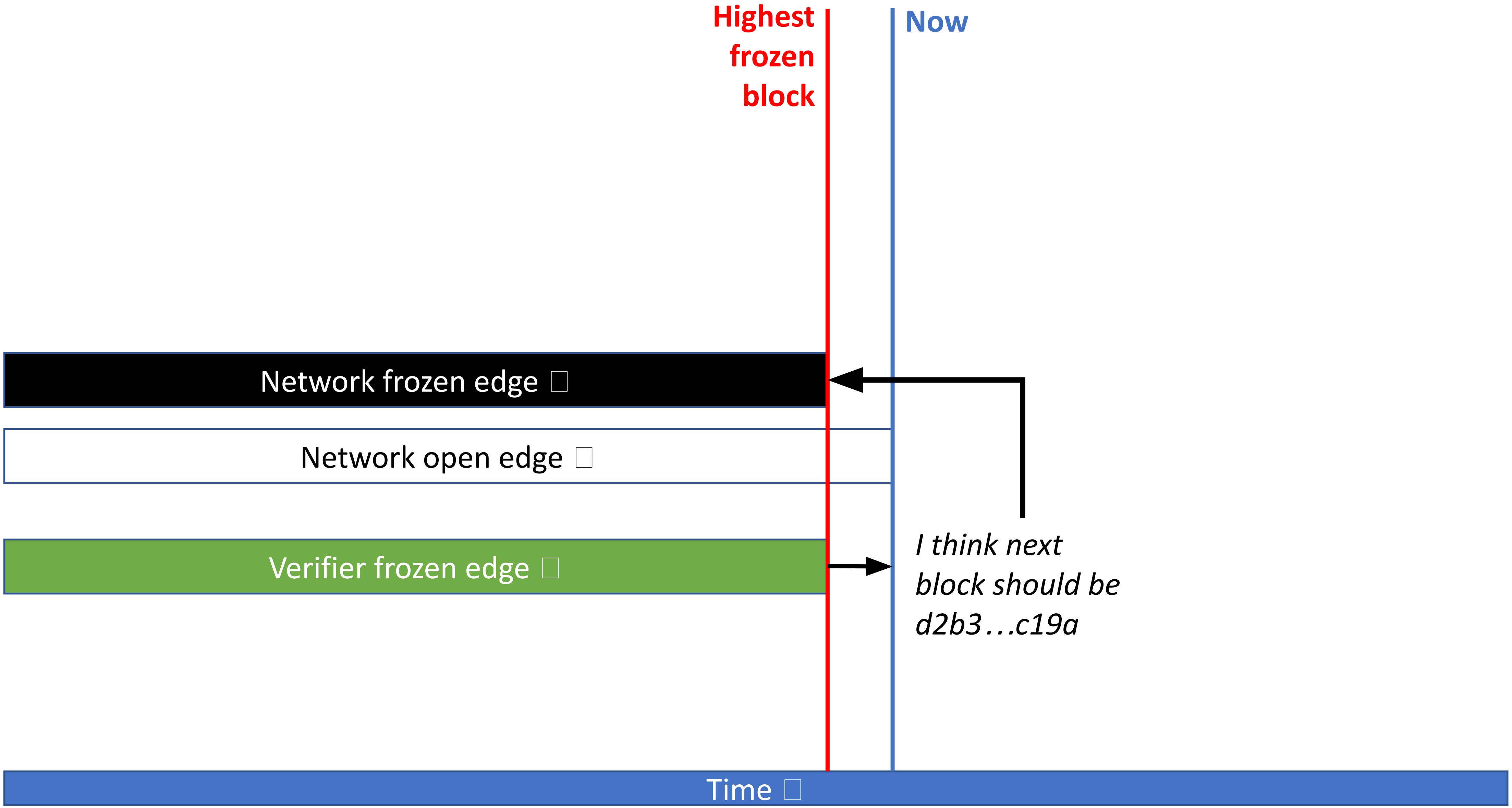
Verifier frozen edge □

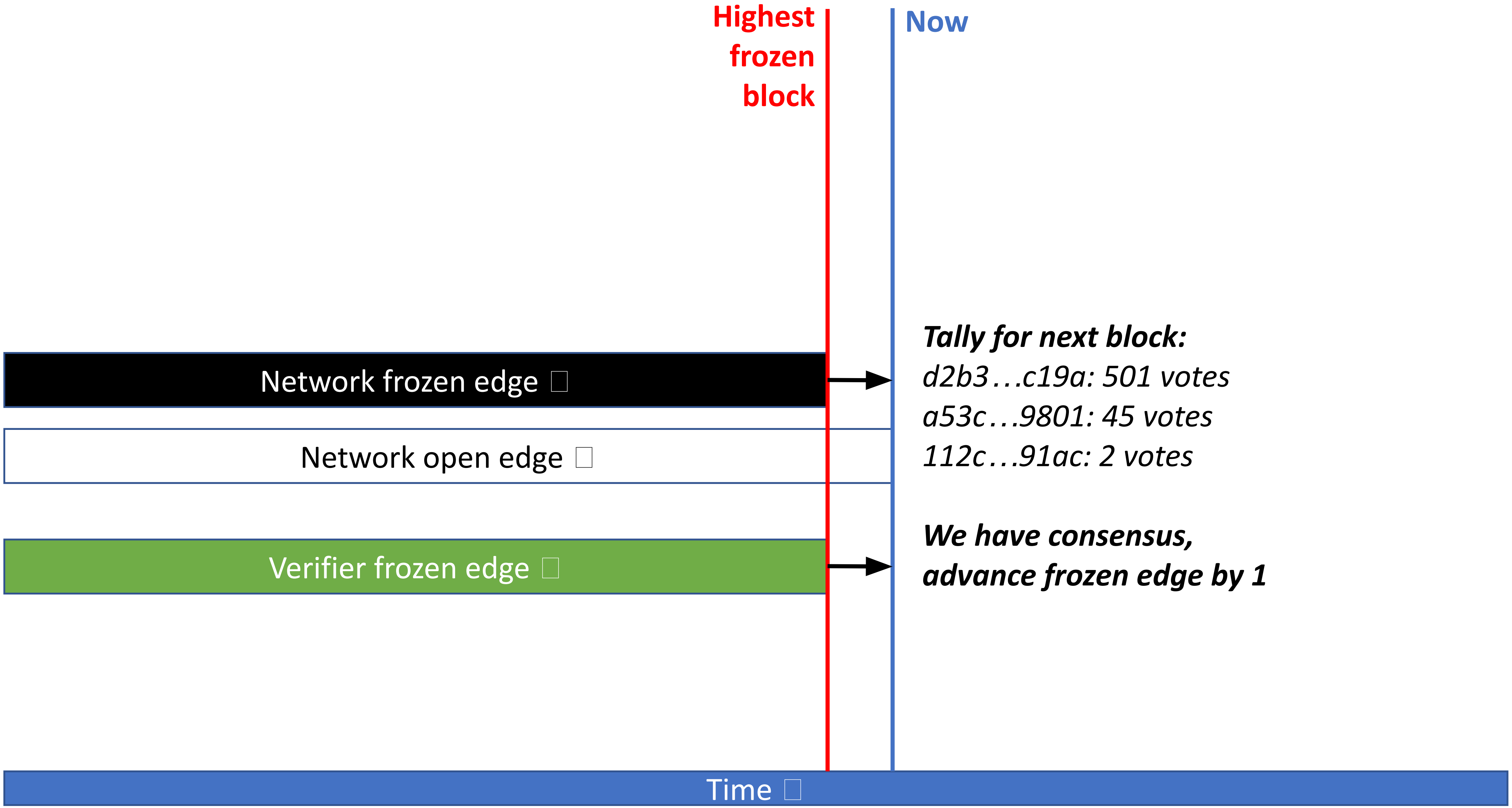
Time □

This verifier is caught up, so it can participate in consensus.

The network is still trying to freeze blocks as fast as possible to catch up to the open edge.

April 2019 update: transactions *can* be timely processed even if the frozen edge has not “caught up”.





Highest frozen block

Now

Network frozen edge □

Network open edge □

Verifier frozen edge □

Time □

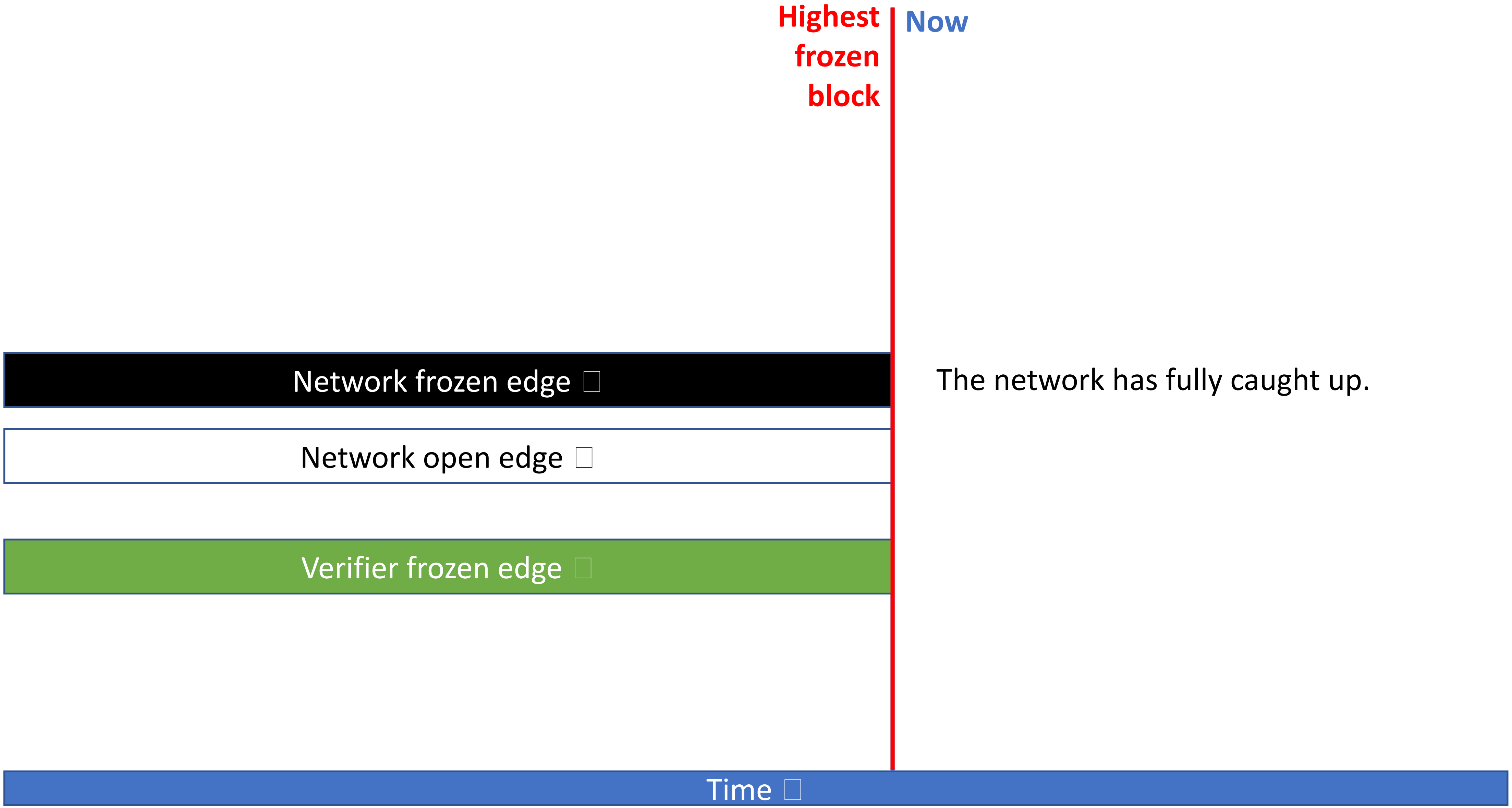
Tally for next block:

d2b3…c19a: 501 votes

a53c…9801: 45 votes

112c…91ac: 2 votes

We have consensus, advance frozen edge by 1



Highest frozen block

Now

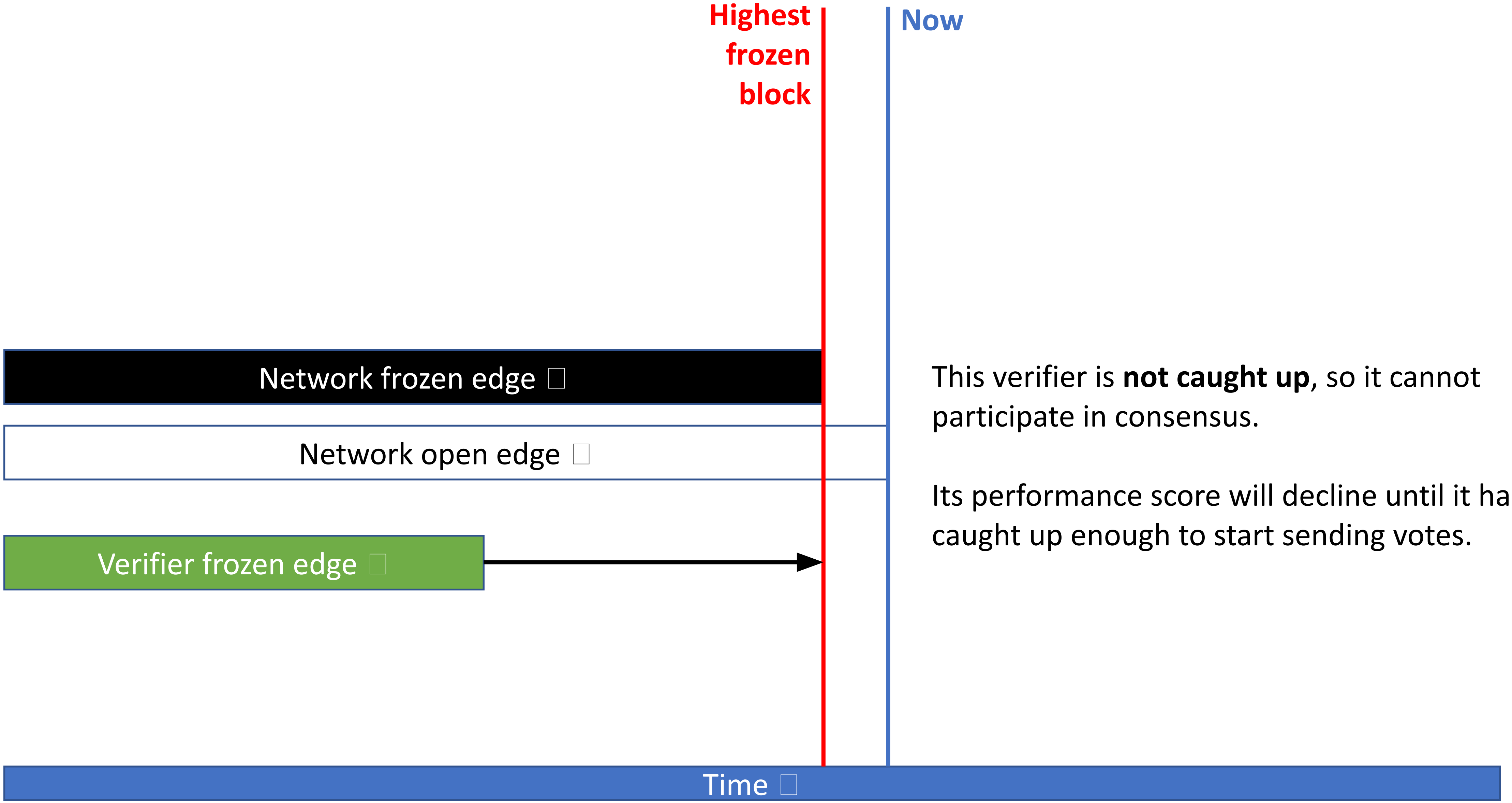
Network frozen edge □

Network open edge □

Verifier frozen edge □

Time □

The network has fully caught up.



Highest frozen block

Now

Network frozen edge □

Network open edge □

Verifier frozen edge □

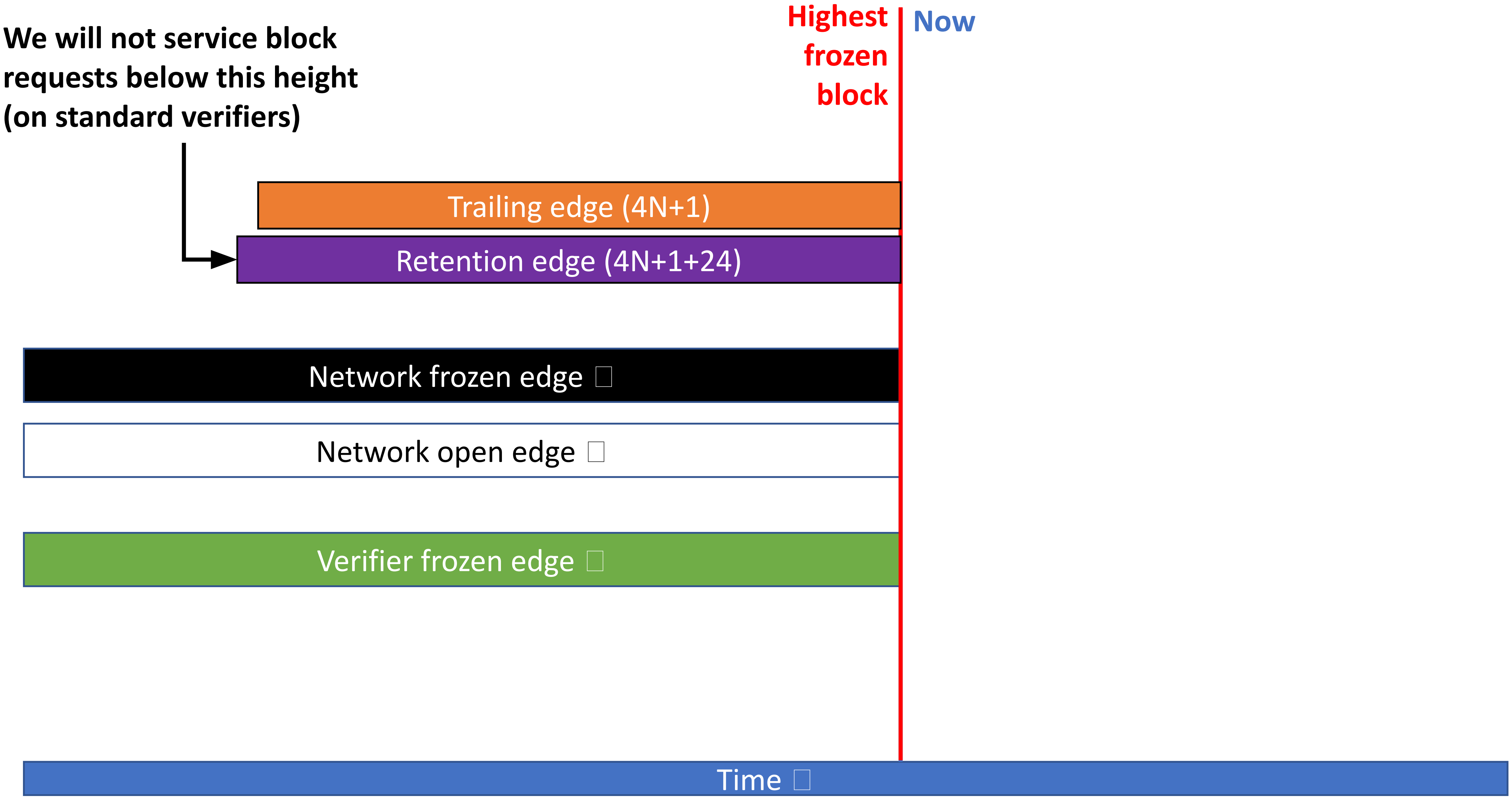
Time □

This verifier is **not caught up**, so it cannot participate in consensus.

Its performance score will decline until it has caught up enough to start sending votes.

Retention and trailing

- To prevent blockchain bloat and improve performance, we only **fully verify the last** 4 cycle's (4N) plus one worth of blocks**.** **T = current – 4N - 1** is the **trailing edge**.
- For some leeway, we set the retention edge slightly before this. **R = T – 24**.
- If we have 1000 blocks with height less than 4N, we compress blocks (**R– 1000**) to (**R**) into a single file. This block only stores the **balance** of all identifiers, so it reduces space by about 99%



We will not service block requests below this height (on standard verifiers)

Highest frozen block

Now

Trailing edge (4N+1)

Retention edge (4N+1+24)

Network frozen edge □

Network open edge □

Verifier frozen edge □

Time □

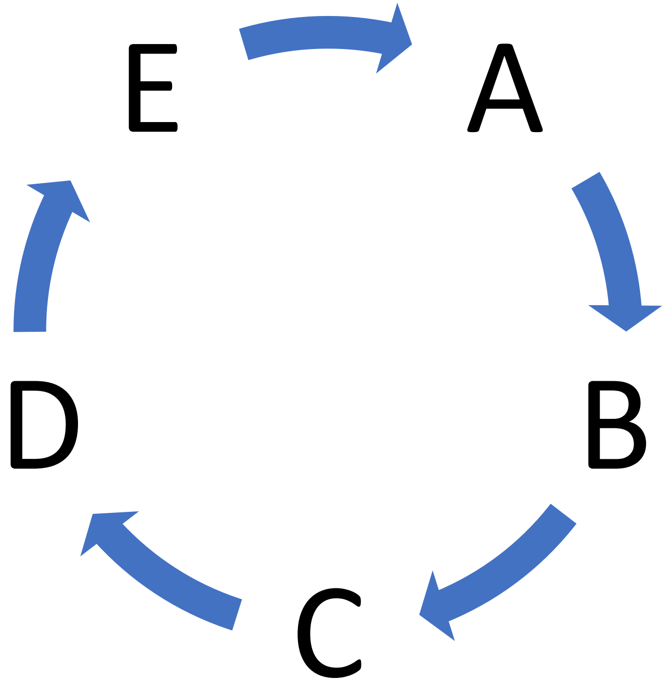
Consensus rules

- **Proof-of-diversity rule 1: After the first existing verifier in the blockchain, a new verifier is only allowed if none of the other blocks in the cycle, the previous cycle, or the two blocks before the previous cycle were verified by new verifiers.**
- **Proof-of-diversity rule 2: Past the Genesis block, the cycle of a block must be longer than half of one more than the maximum of the all cycle lengths in this cycle and the previous two cycles.**

(https://nyzo.co/whitepaper)

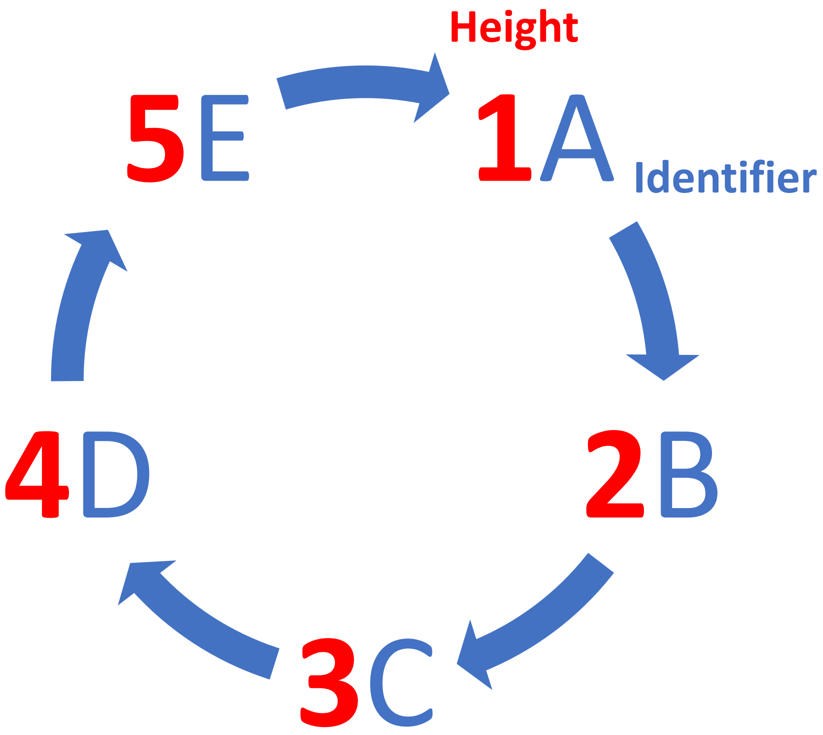
Proof of diversity rule 1

- Verification cycle (mesh of size 5):



Proof of diversity rule 1

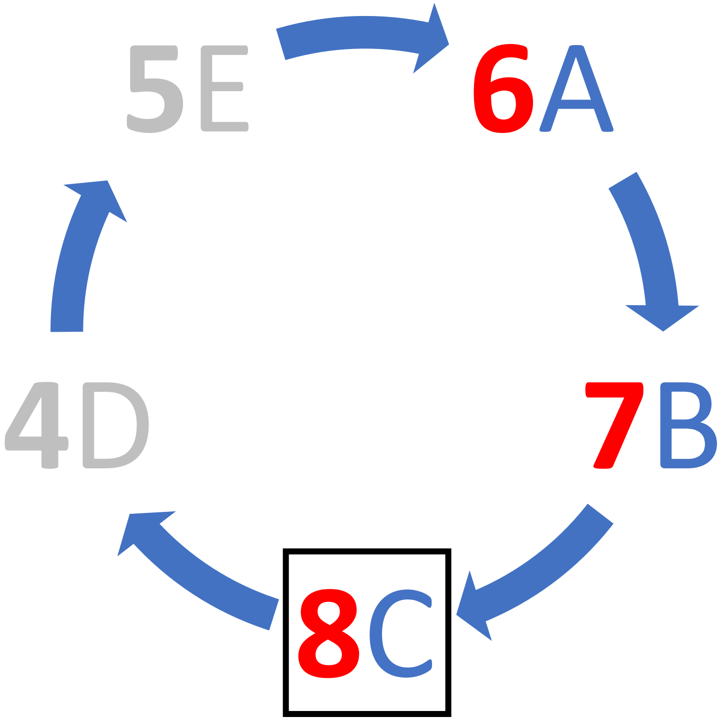
- Verification cycle (mesh of size 5):



Height: 5

Proof of diversity rule 1

- Verification cycle (mesh of size 5):

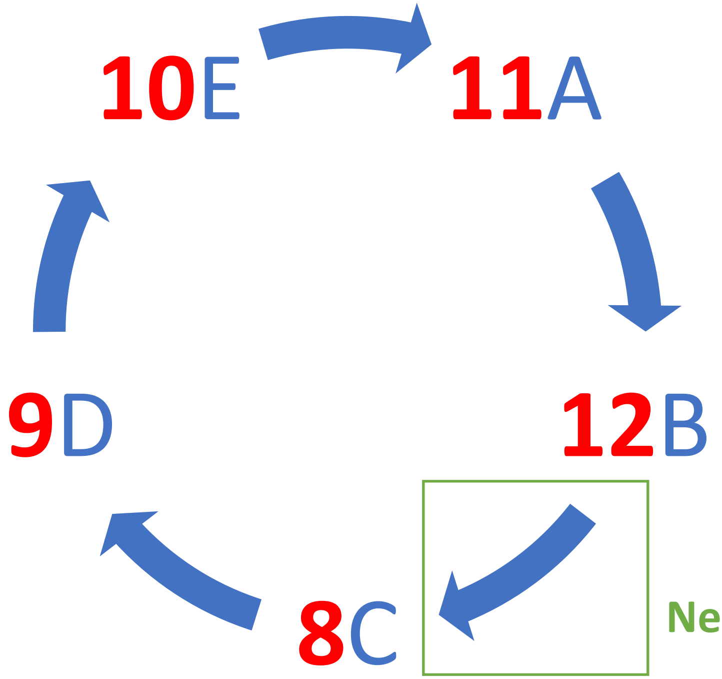


Verification cycle for block 8: <u>8C, 7B, 6A, 5E, 4D</u>

Height: 8

Proof of diversity rule 1

- Verification cycle (mesh of size 5):

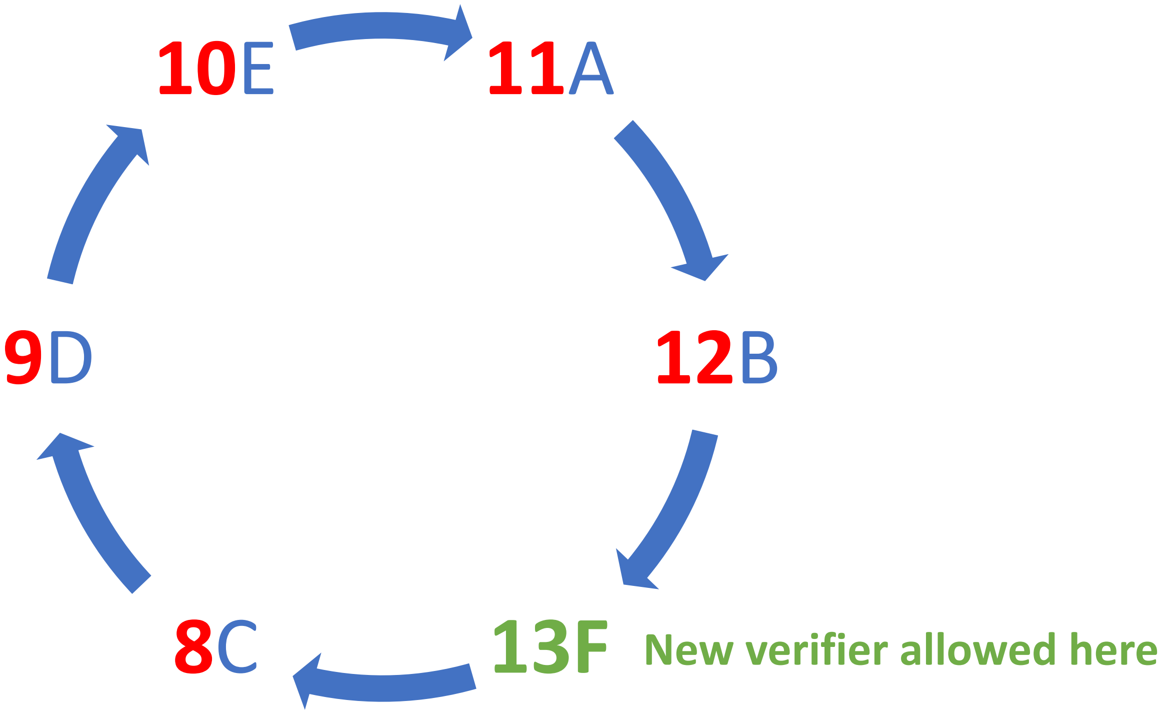


New verifier allowed here

Height: 12

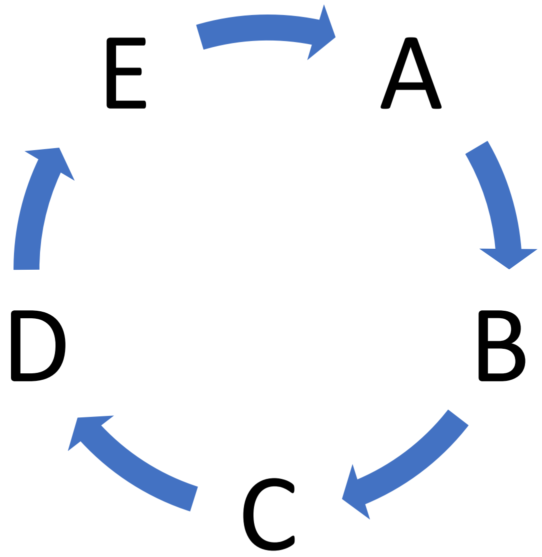
Proof of diversity rule 1

- Verification cycle (mesh of size 6):

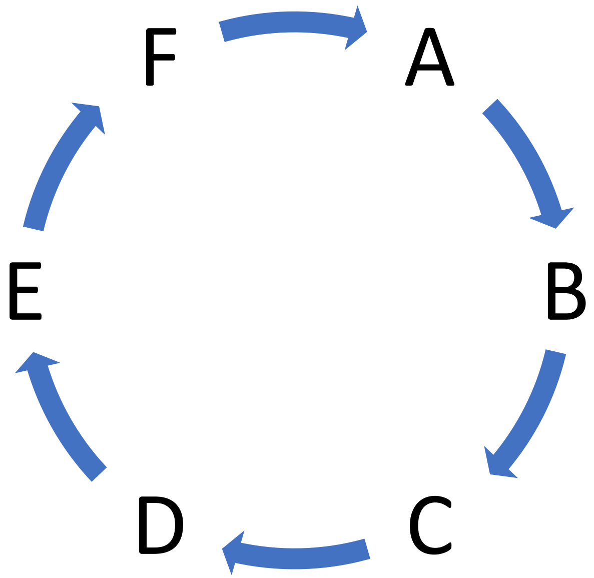


Height: 13

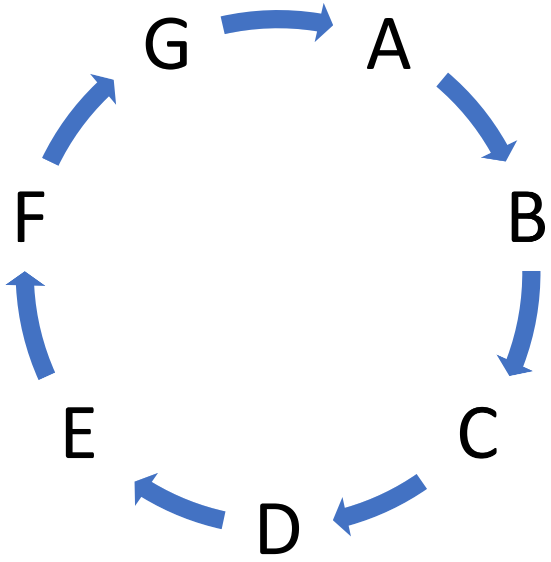
Proof of diversity rule 2



$C_{n-2}=5$



$C_{n-1}=6$



$C_n=7$

Proof of diversity rule 2

$$C_{n+1} > ½ [\max(C_{n-2}, C_{n-1}, C_n) + 1]$$

$C_{n+1} > 4$ (next cycle must be at least 4 verifiers in length)

$C_{n-2}=5$ $C_{n-1}=6$ $C_n=7$

Incentive system and economic rationale

- If you want coins, you have two options: joining the verification cycle or helping to improve the system by finding and reporting bugs.
- If you are able to join the cycle as a verifier, you get 10% of the transaction fees for each block you verify and 10% of transaction fees for each of the next 9 blocks in the chain. This is how you will earn coins at the beginning, and this is how you will continue to earn coins as more people join the system. Unlike mined currencies, we're not going to have a drop-off of profitability as time goes on. As more people join the network, more transaction fees should be generated. These fees will be split among a larger pool of people as more verifiers join, but the blockchain rules limit the growth rate of the cycle to an inverse proportion of the cycle length. With a cycle length of 500, fewer than 13 verifiers can be added each day. With a cycle length of 1000, fewer than 7 verifiers can be added each day.

(https://nyzo.co/whitepaper)

Incentive system and economic rationale

- All transactions incur a 0.25% fee. This fee is split evenly among the verifier of this block and the verifiers of the previous nine blocks. For blocks before block 9, the fee is split evenly among the verifier of this block and all previous blocks. Transaction fees that cannot be divided evenly are rounded down to the nearest micronyzo, and the remainder is rolled over to the next block.

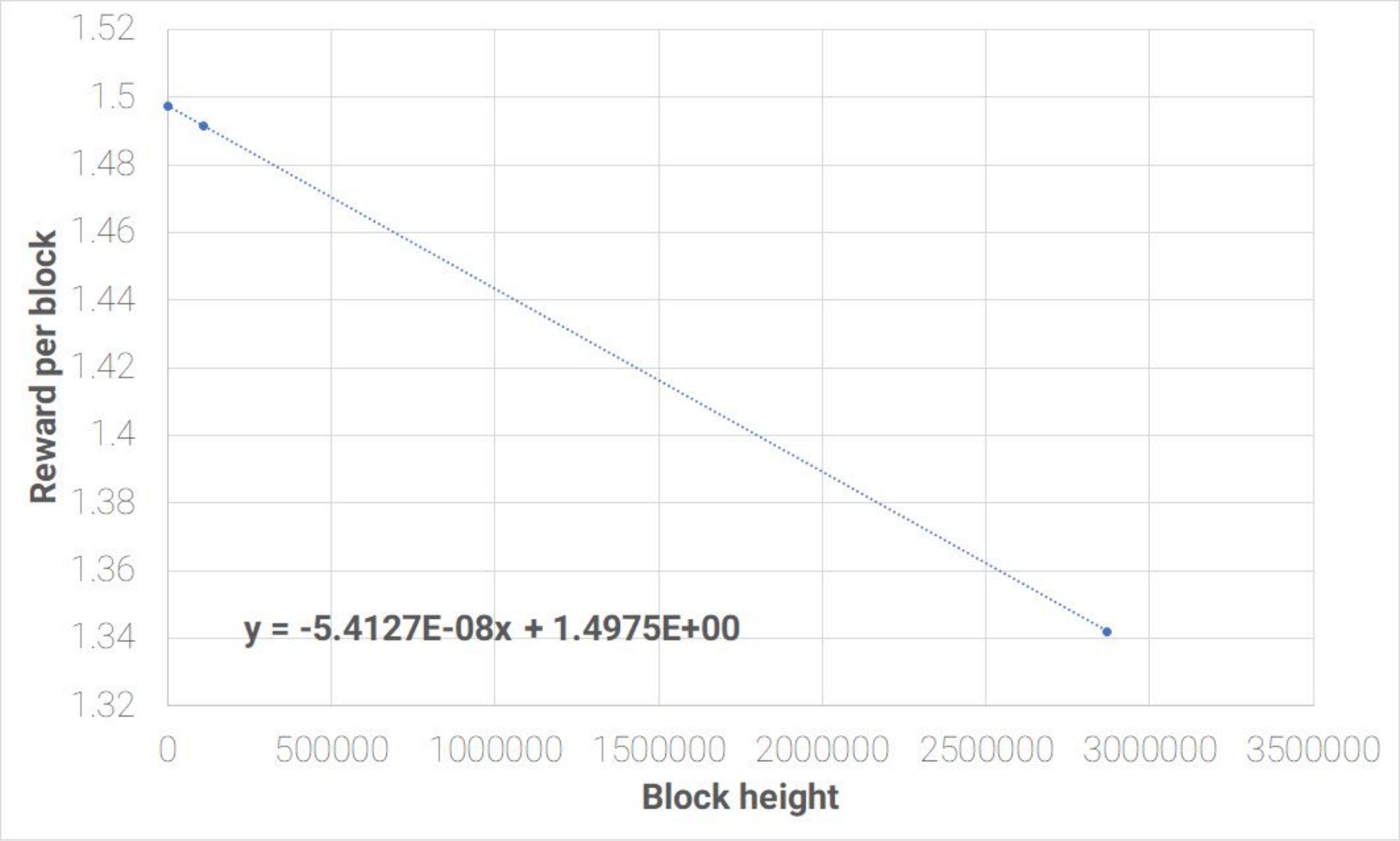
(https://nyzo.co/whitepaper)

Incentive system and economic rationale

- **<u>Overview of incentive system:</u>**
  - **<u>20,000,000 nyzos (20%) are allocated to seed transactions for the next 5 years</u>**
  - These transactions simulate on-chain network activity, and transactions fees given to verifiers in the cycle
  - The seed transactions serve no other purpose.

Incentive system and economic rationale

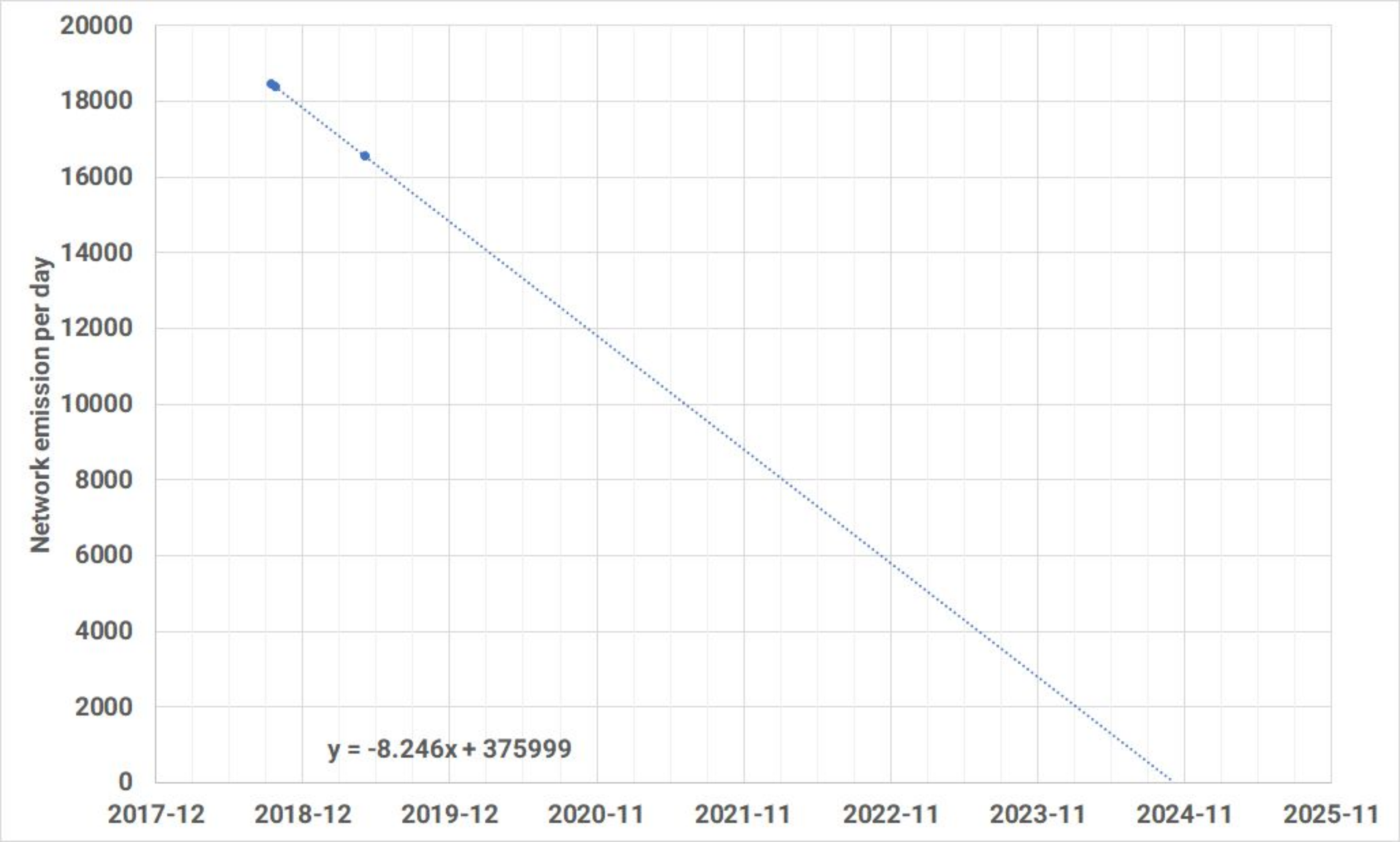
Reward per block = $-5.4127*10^{-8}$ * (block height) + 1.4975



Amount greater than this due to collected transaction fees

Incentive system and economic rationale

Network emission per day = -8.426 * (date) + 375999



Note that this value is (strongly) invariant to the number of verifiers queued or active

Amount greater than this due to collected transaction fees