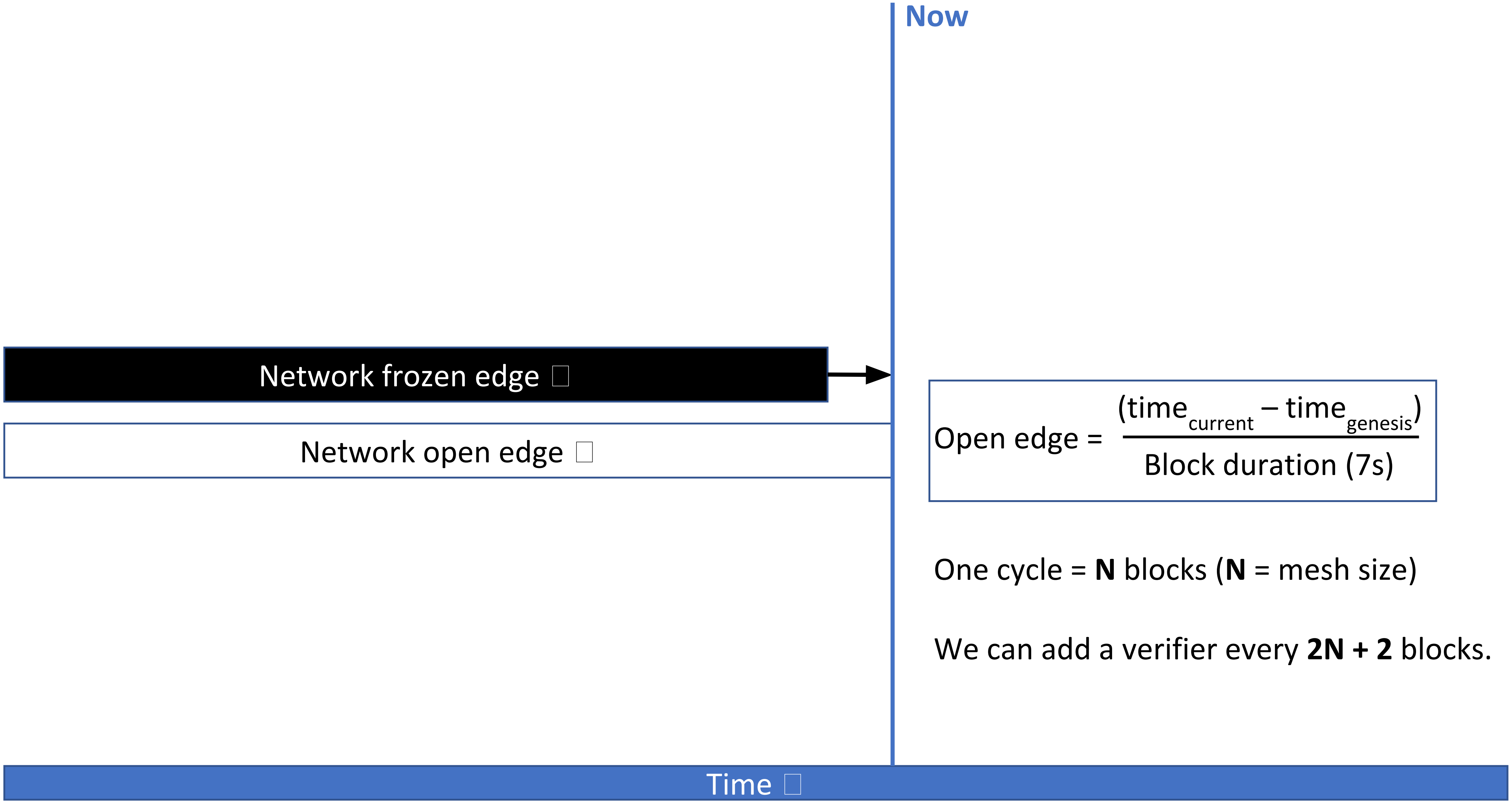
Nyzo design document v0.3

@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



Now

Network frozen edge □

Network open edge □

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

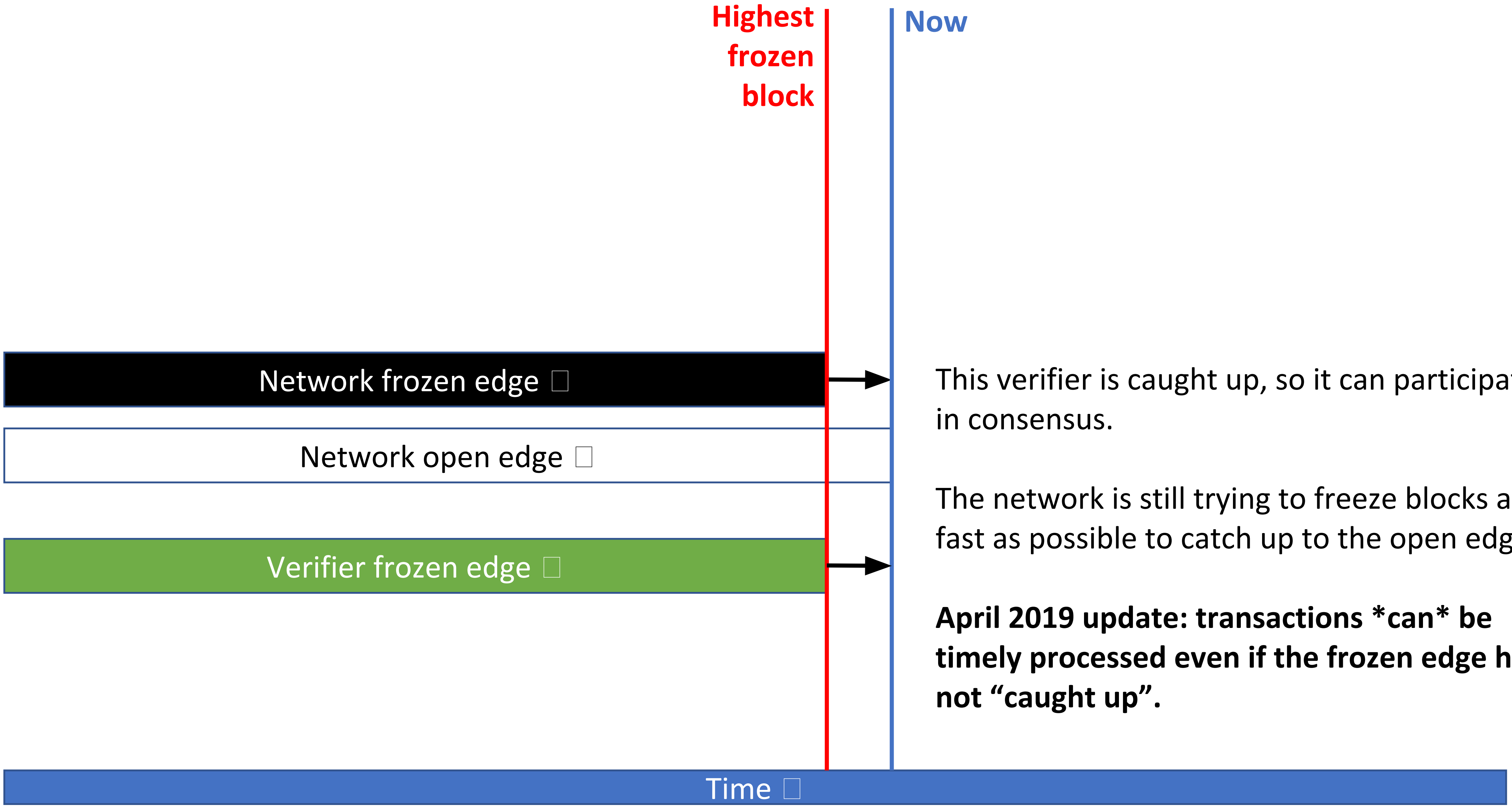
One cycle = **N** blocks (**N** = mesh size)

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

Time □

Network and verifier

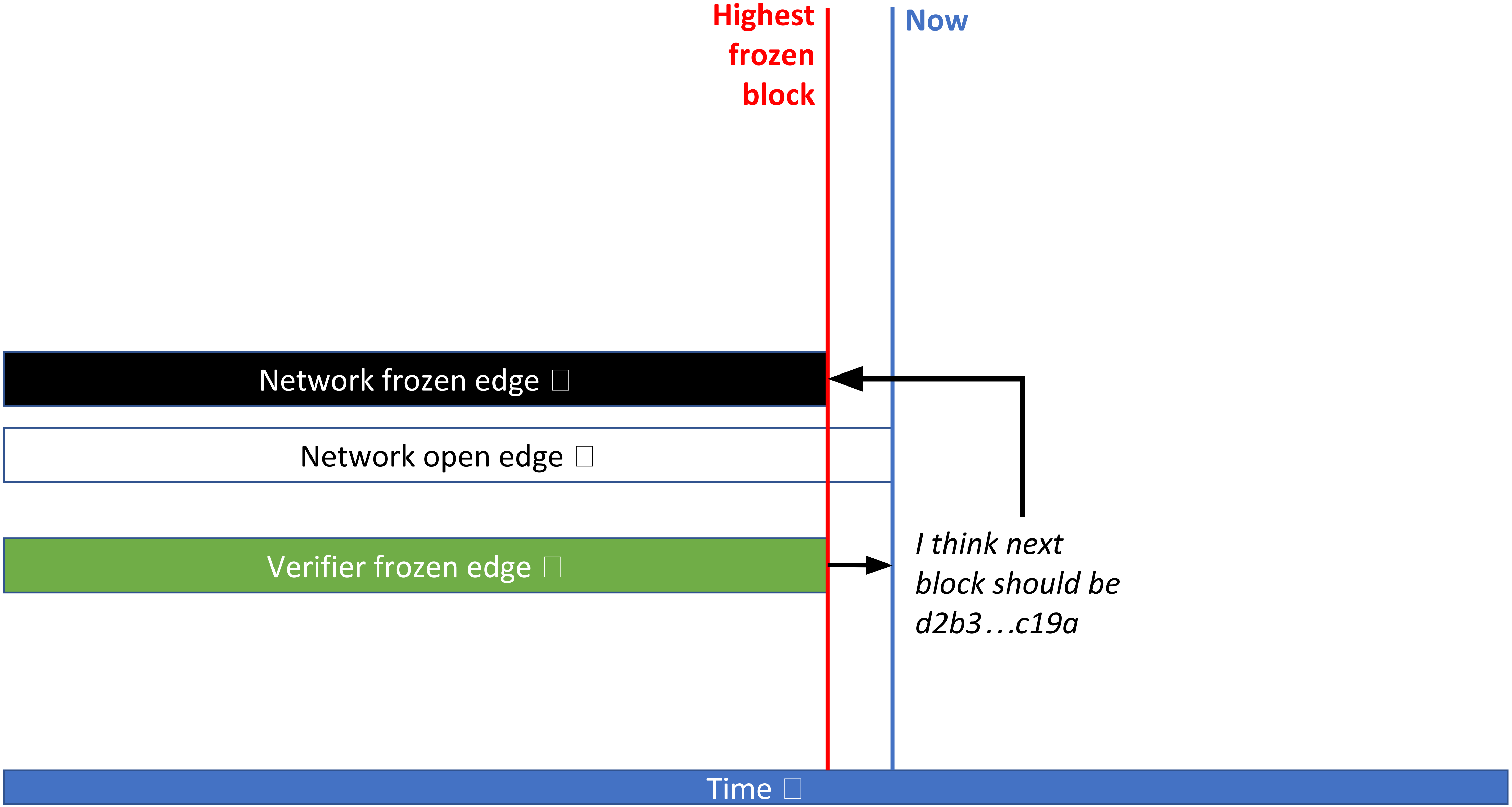
- Verifiers acquire blocks as fast as possible to match the network’s **frozen edge**
- When the frozen edge is caught up, verifiers can vote for the next **block hash**



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

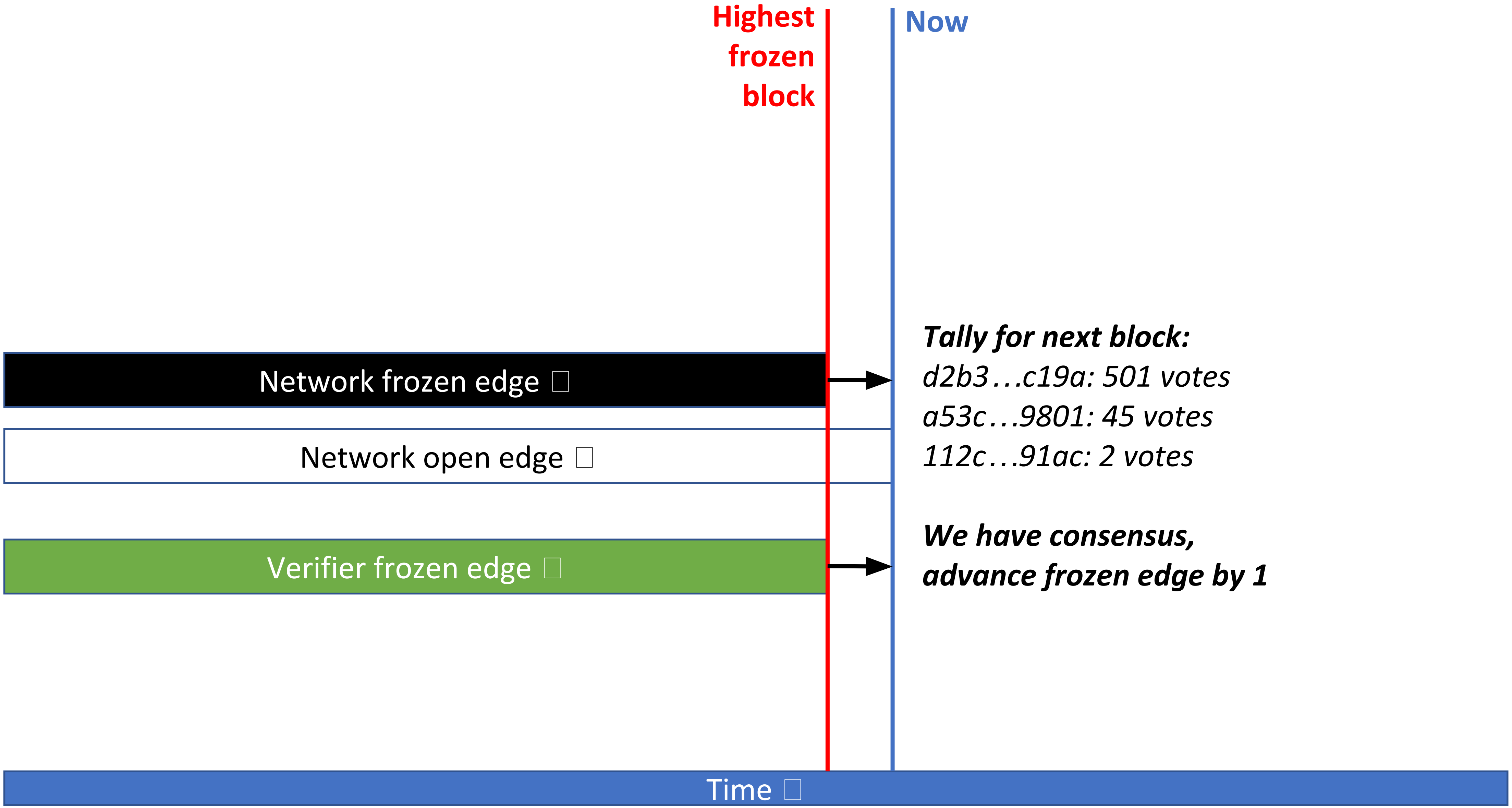
Network frozen edge □

Network open edge □

Verifier frozen edge □

I think next block should be d2b3…c19a

Time □



Highest frozen block

Now

Network frozen edge □

Network open edge □

Verifier frozen edge □

Time □

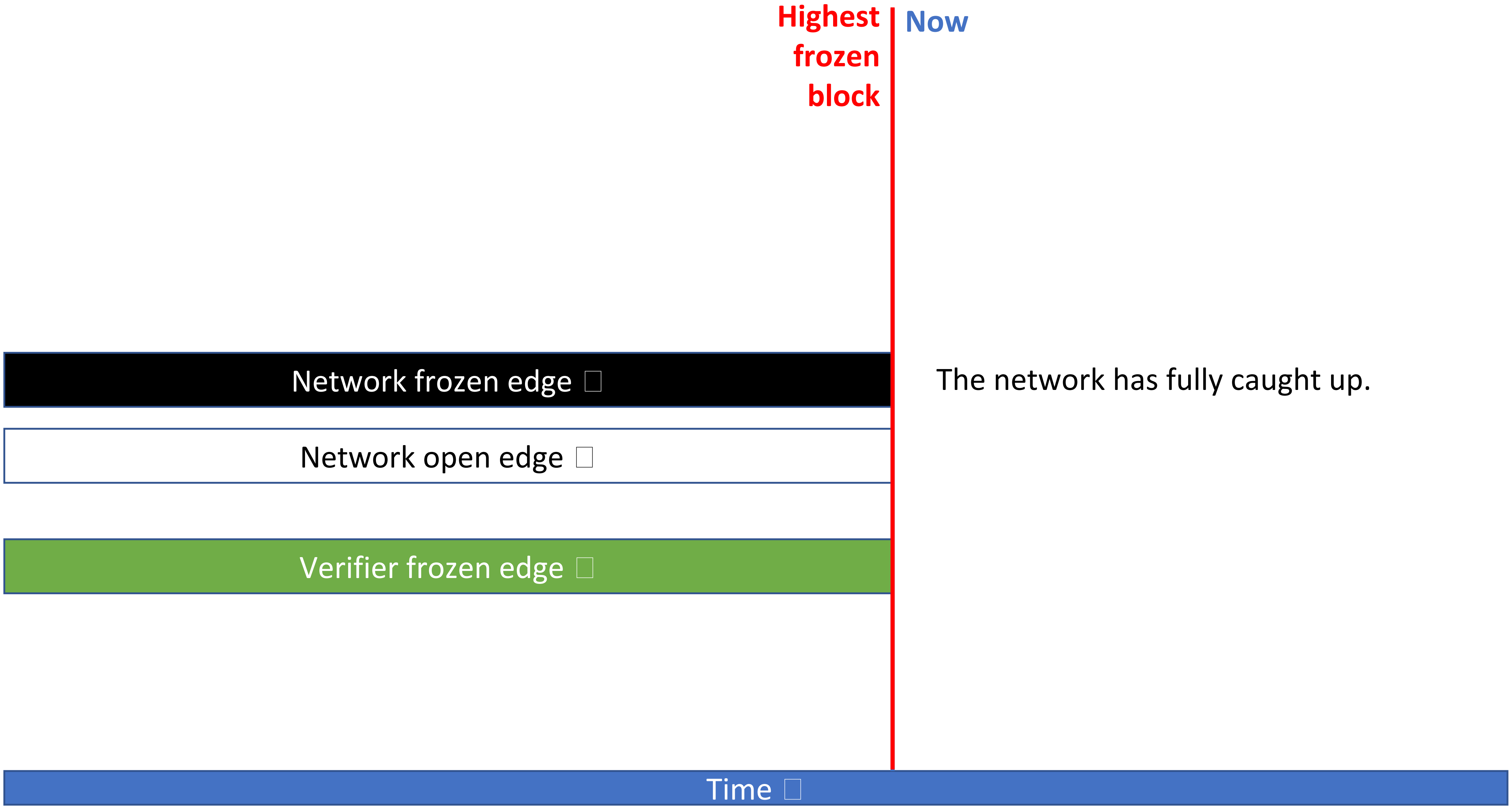
Tally for next block:

d2b3…c19a: 501 votes

a53c…9801: 45 votes

112c…91ac: 2 votes

We have consensus, advance frozen edge by 1



Highest frozen block

Now

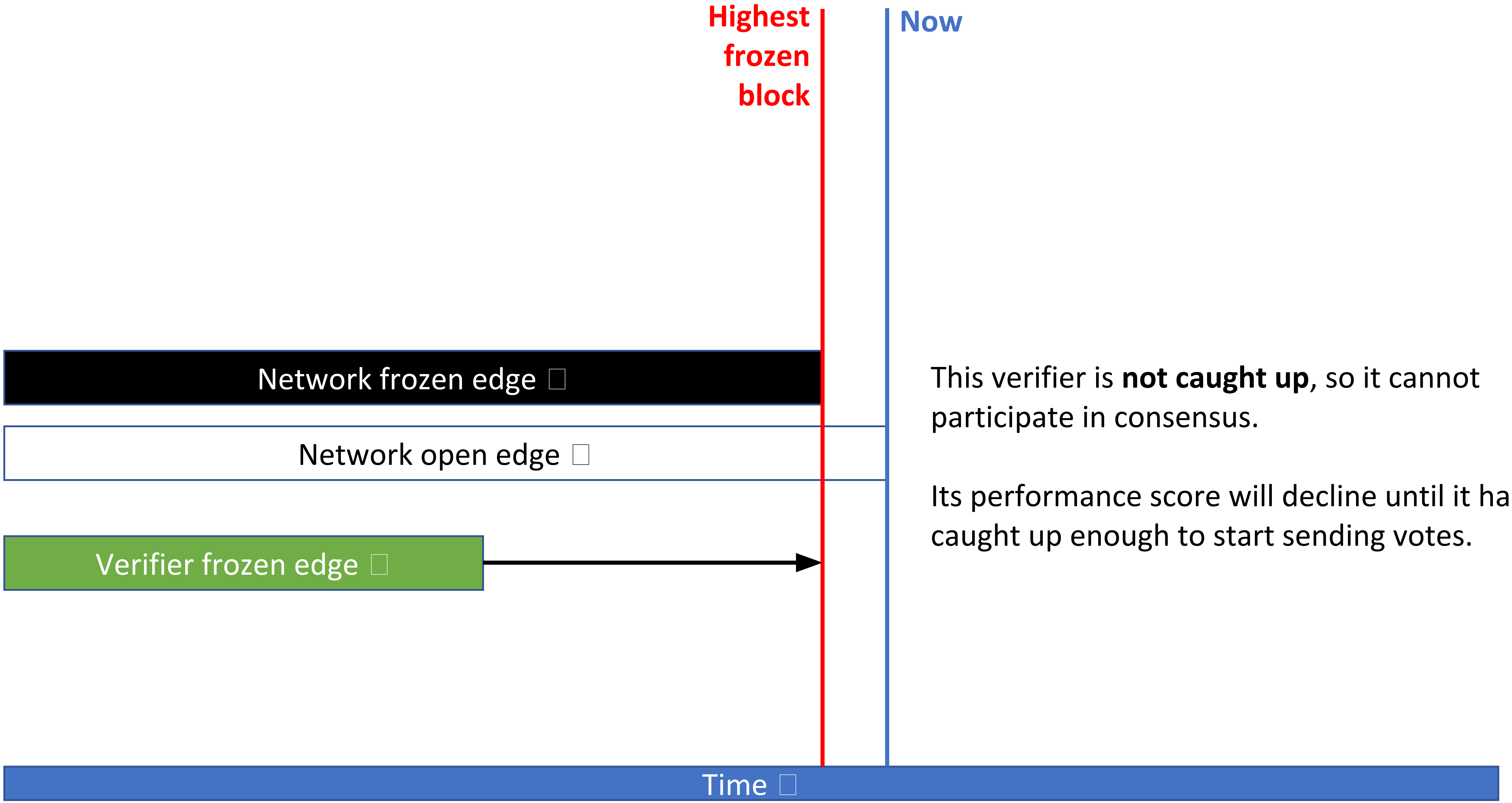
Network frozen edge □

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 □

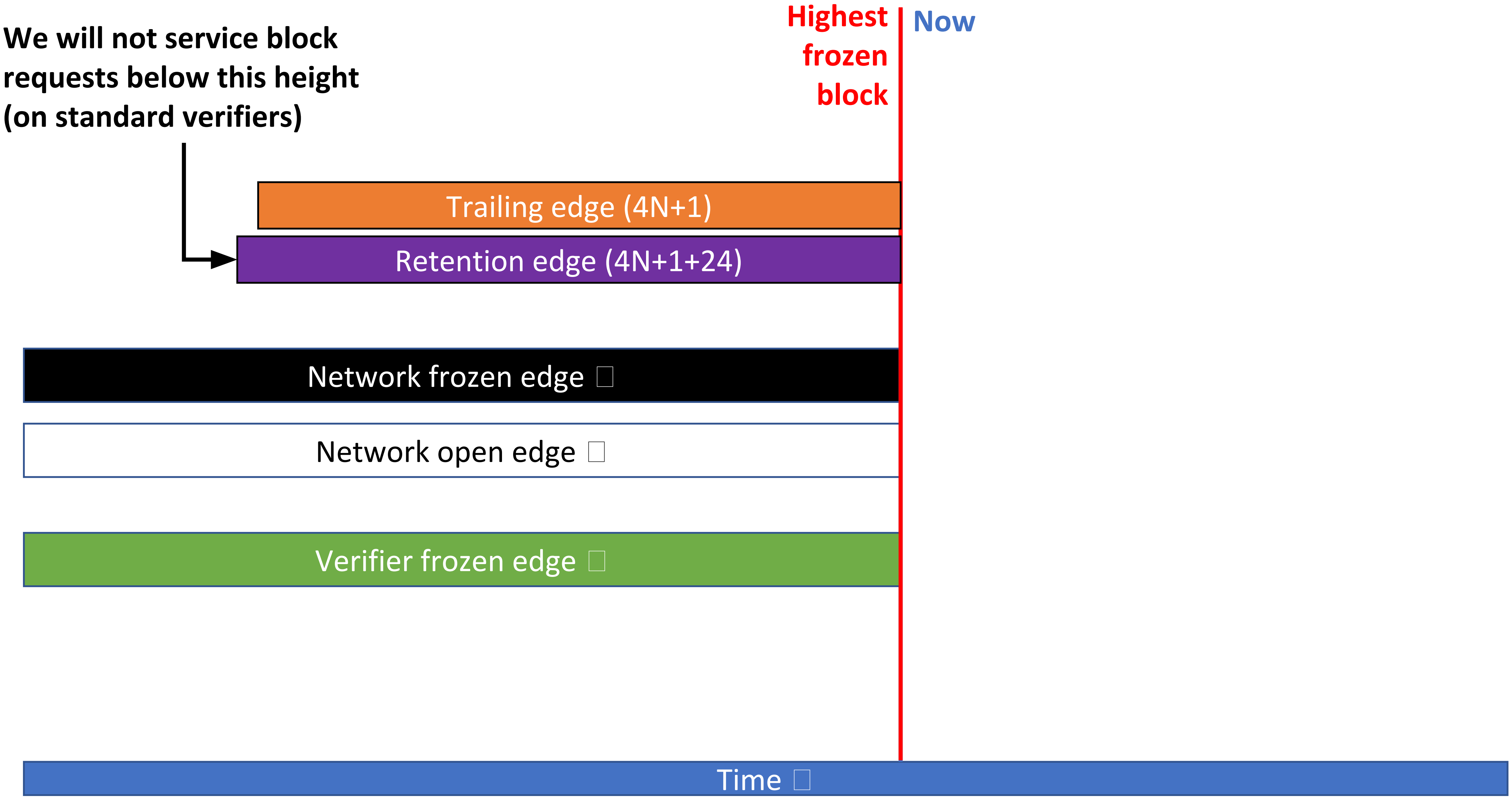
Time □

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 □

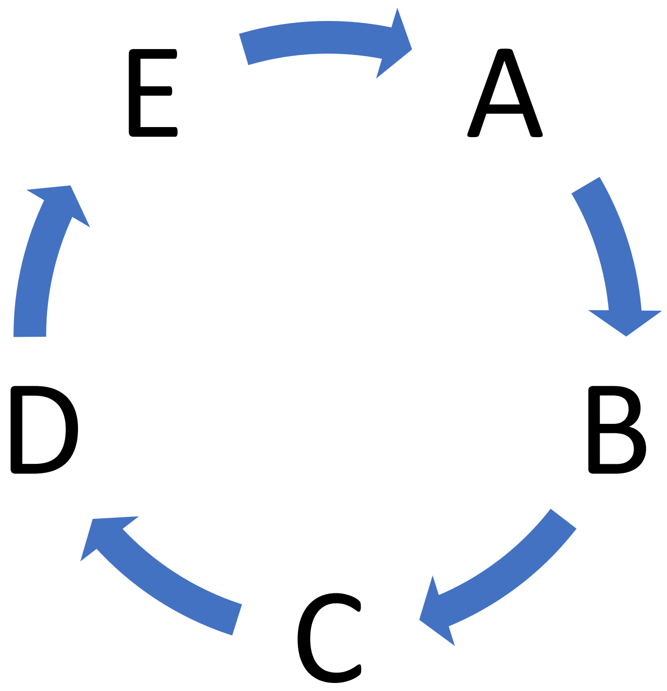
Consensus rules

- 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)

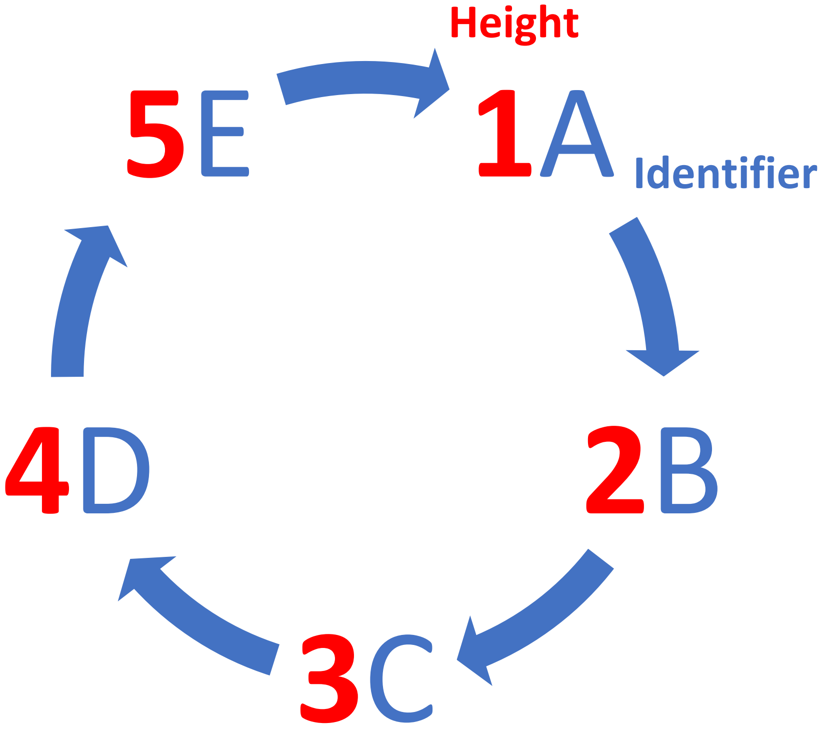
Proof of diversity rule 1

- Verification cycle (mesh of size 5):



Proof of diversity rule 1

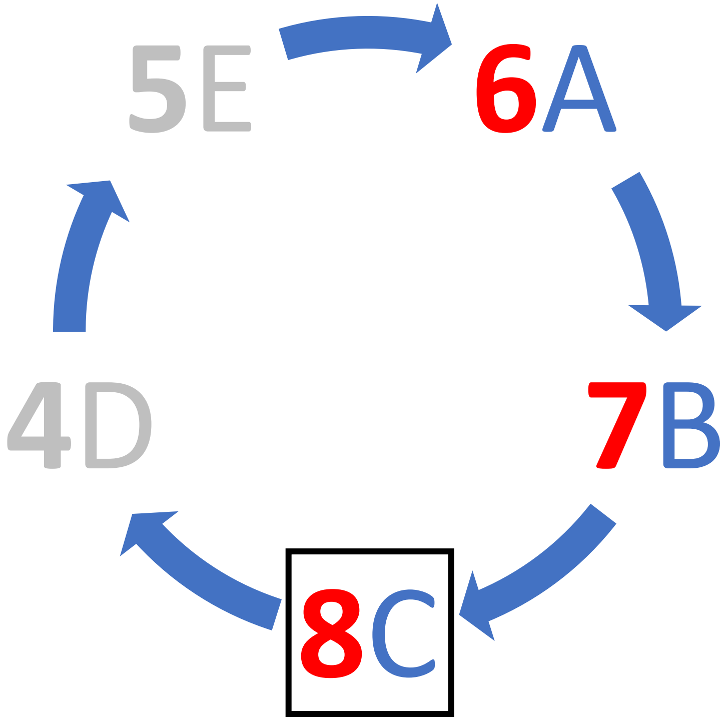
- Verification cycle (mesh of size 5):



Height: 5

Proof of diversity rule 1

- Verification cycle (mesh of size 5):

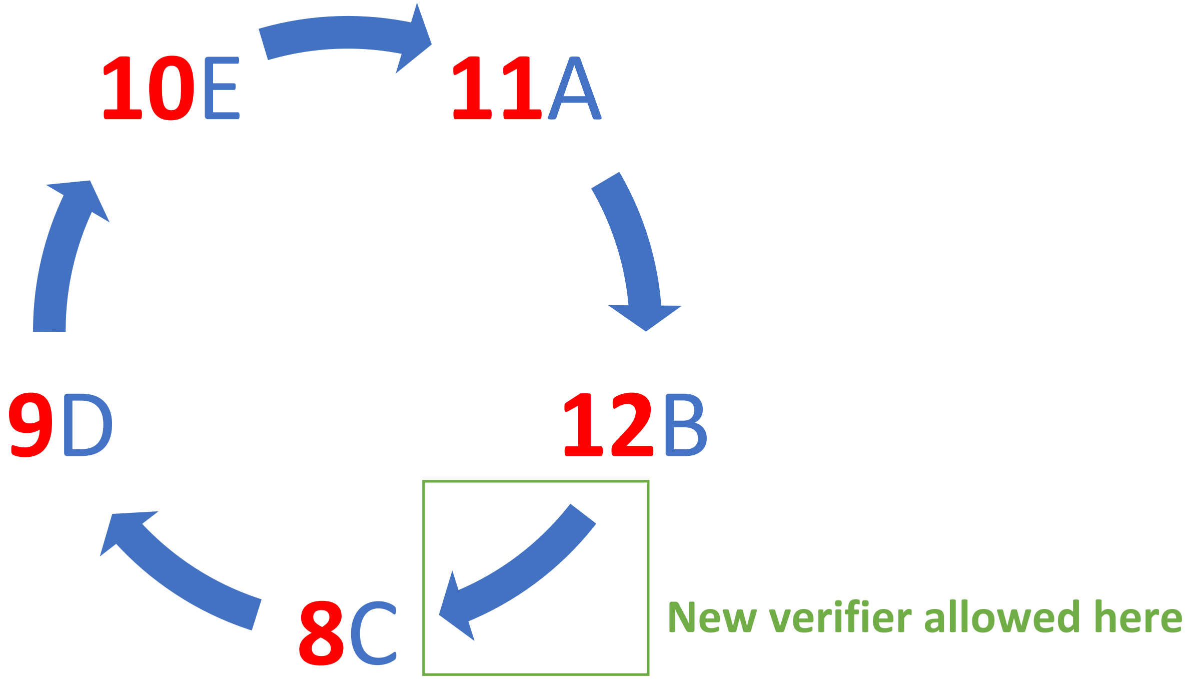


Verification cycle for block 8: <u>8C, 7B, 6A, 5E, 4D</u>

Height: 8

Proof of diversity rule 1

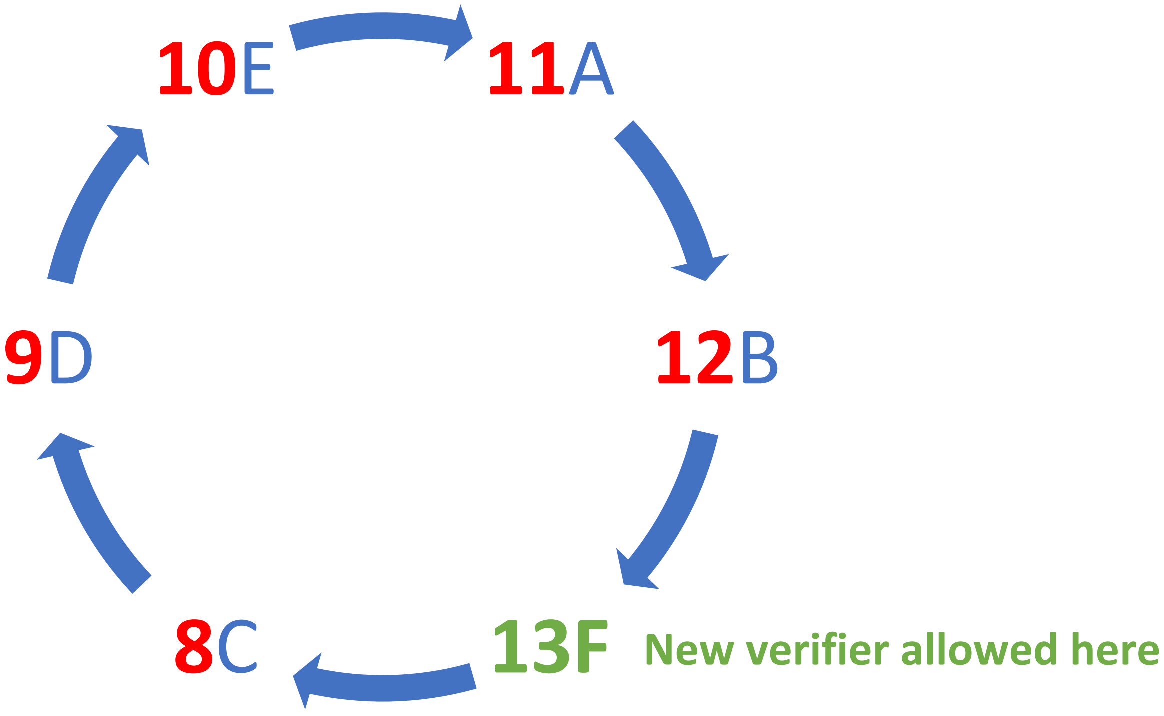
- Verification cycle (mesh of size 5):



Height: 12

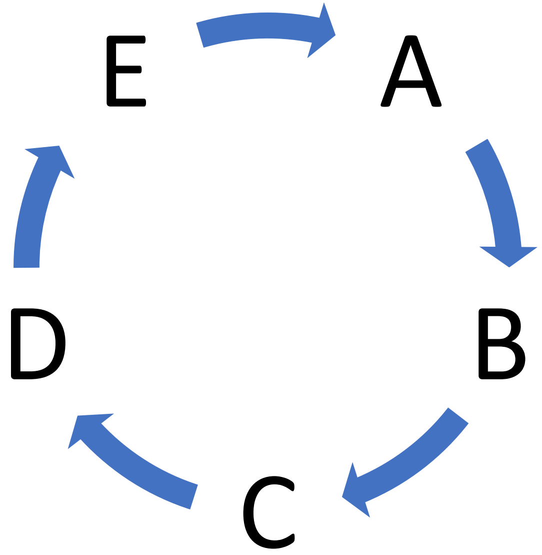
Proof of diversity rule 1

- Verification cycle (mesh of size 6):

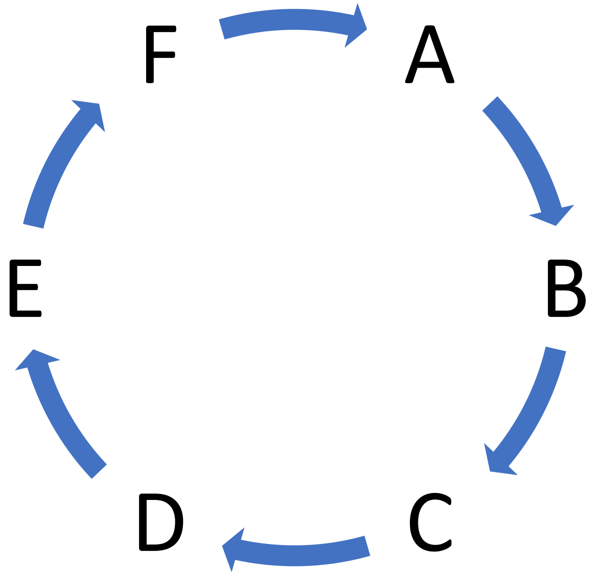


Height: 13

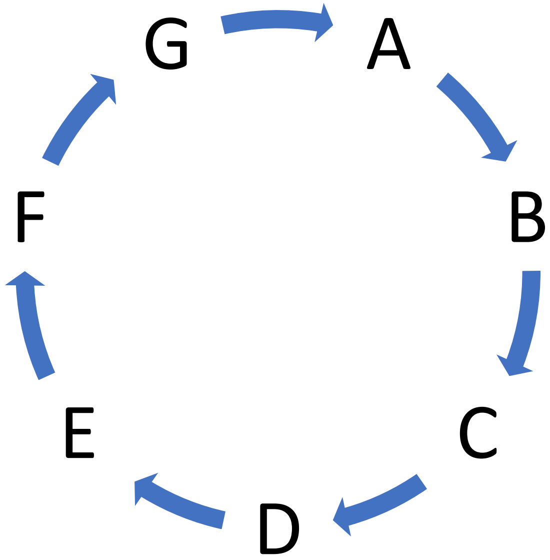
Proof of diversity rule 2



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.

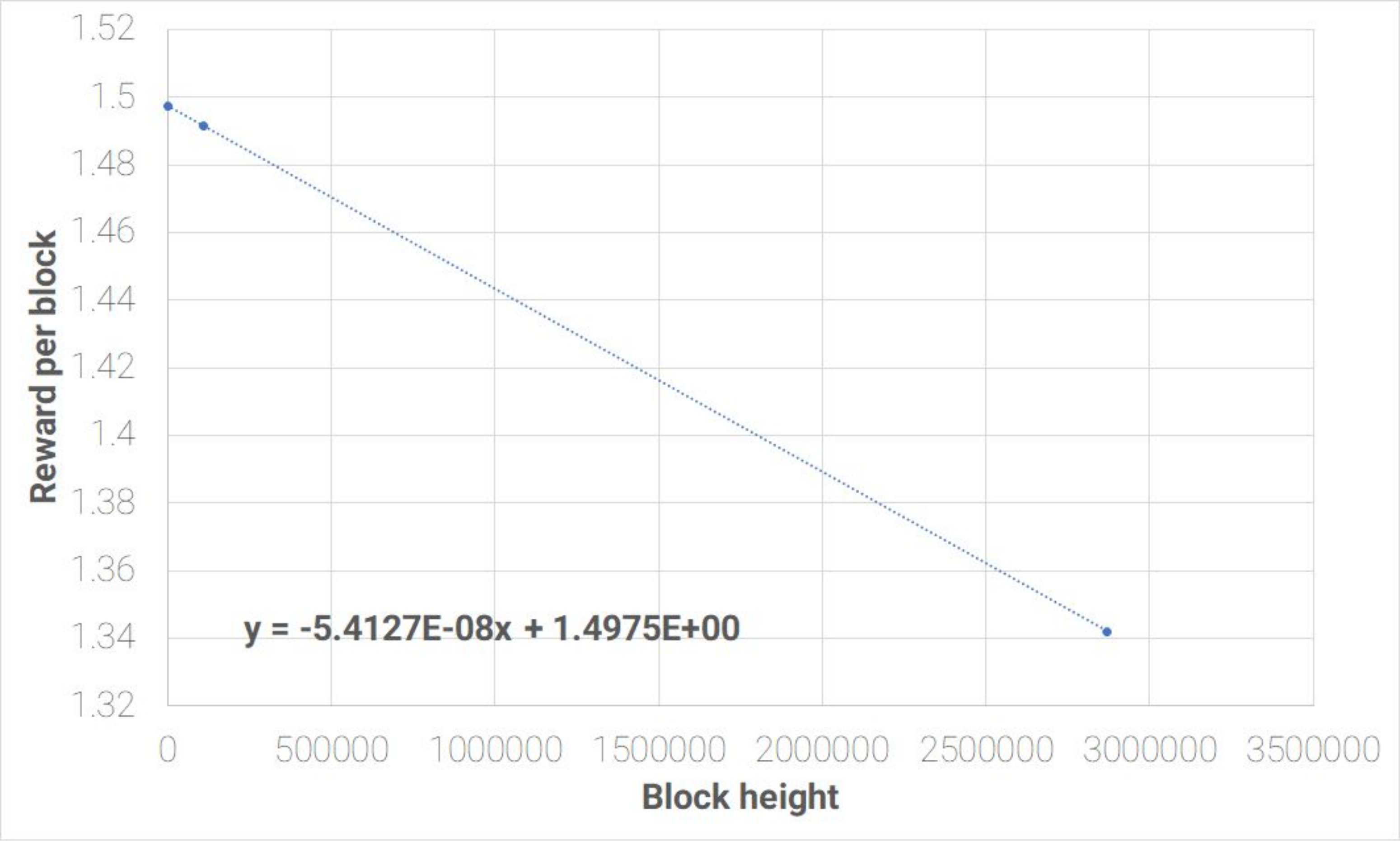
(https://nyzo.co/whitepaper)

Incentive system and economic rationale

- **Overview of incentive system:**
  - **20,000,000 nyzos (20%) are allocated to seed transactions for the next 5 years**
  - 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

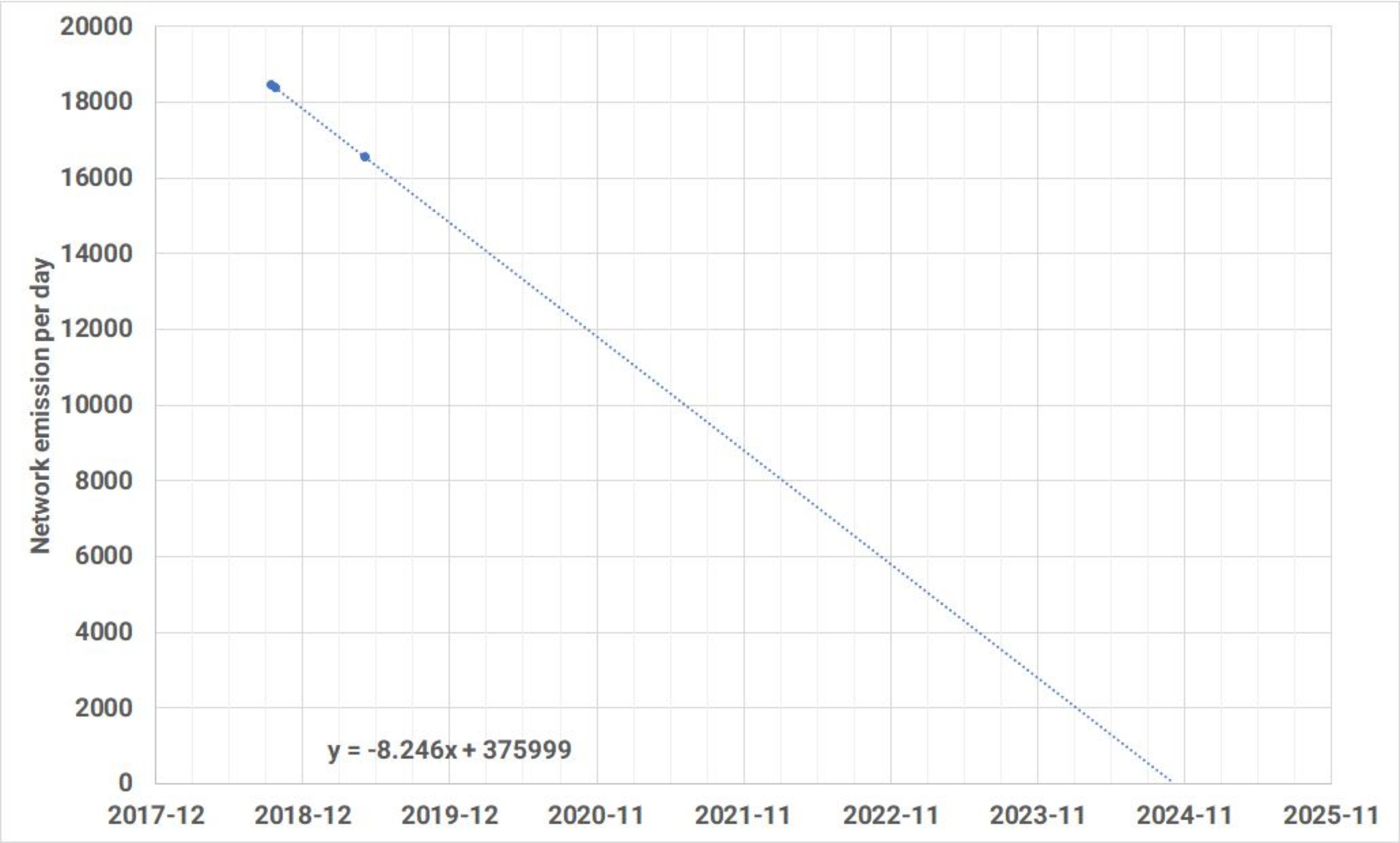
Reward per block = -5.4127*10^{-8} * (block height) + 1.4975



Amount greater than this due to collected transaction fees

Incentive system and economic rationale

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

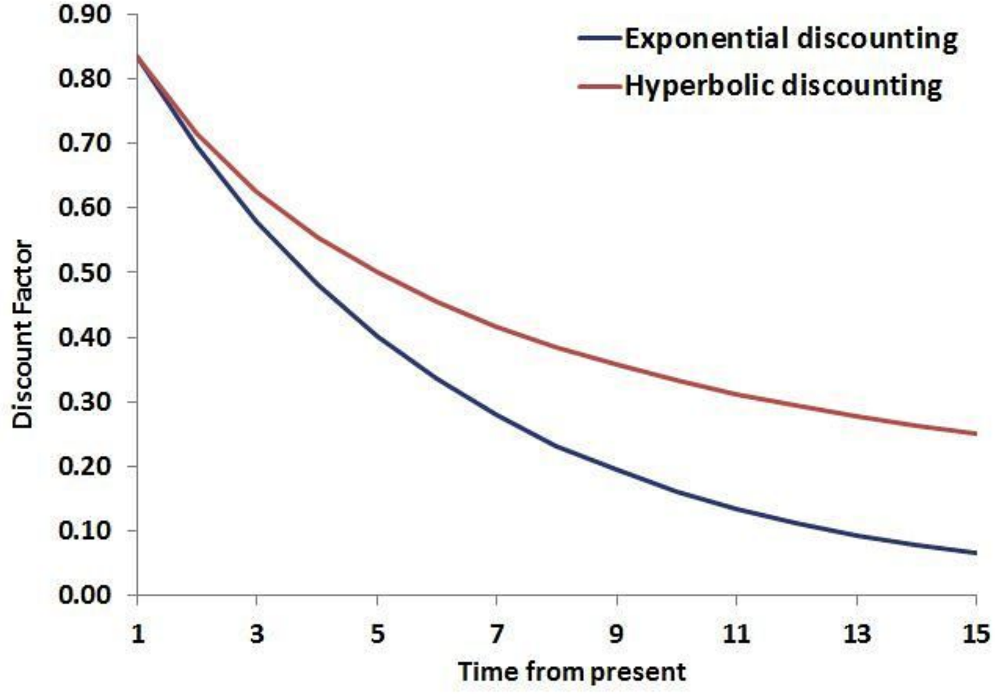


Note that this value is (strongly) invariant to the number of verifiers queued or active

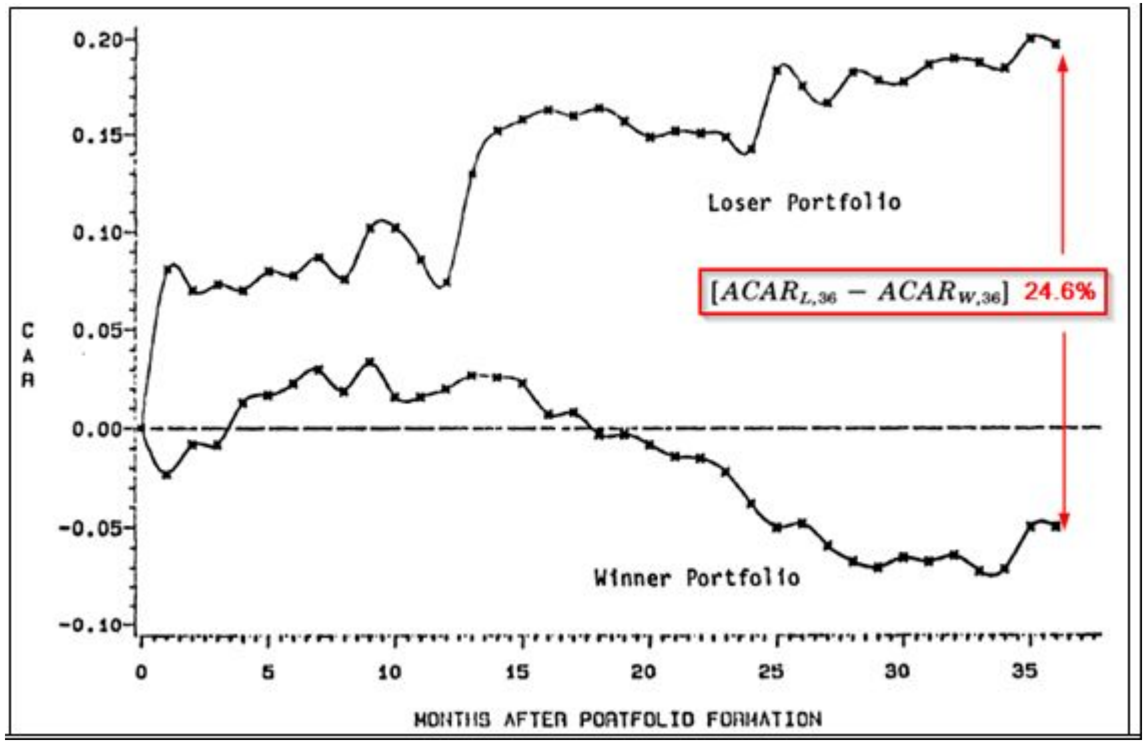
Amount greater than this due to collected transaction fees

Incentive system and economic rationale

Humans are subject to behavioral biases:



Hyperbolic discounting



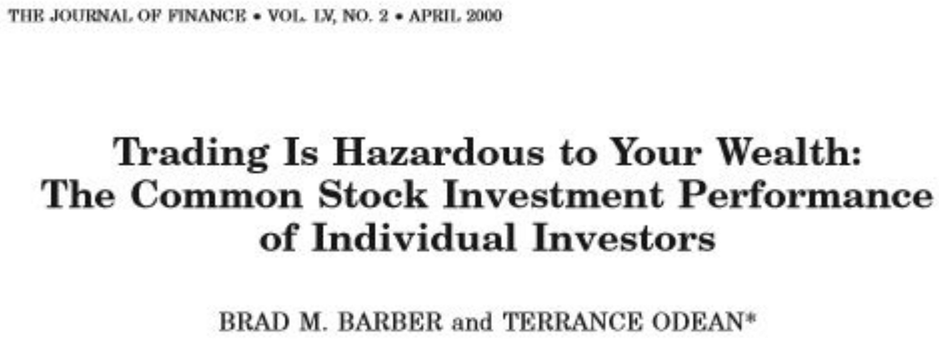
Overreaction (value and momentum)

Incentive system and economic rationale

Behavioral biases are costly:

Timing Poorly: A Guide to Generating Poor Returns While Investing in Successful Strategies

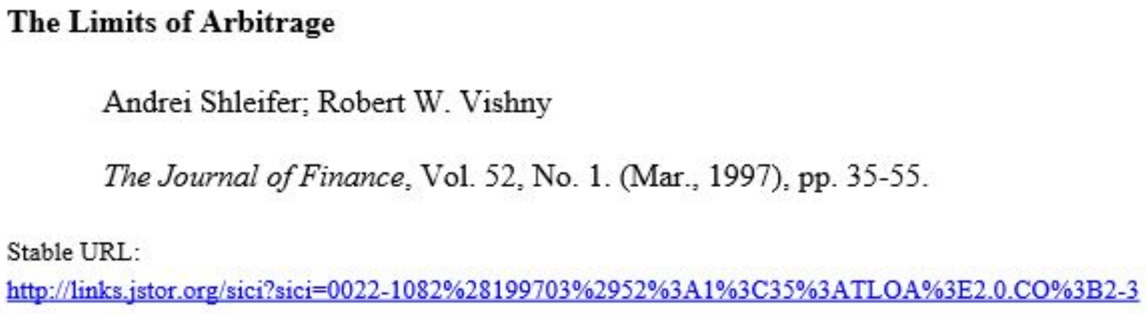
Jason Hsu
Research Affiliates, LLC
UCLA Anderson School of Management



THE JOURNAL OF FINANCE • VOL. LV, NO. 2 • APRIL 2000

Trading Is Hazardous to Your Wealth: The Common Stock Investment Performance of Individual Investors

BRAD M. BARBER and TERRANCE ODEAN*

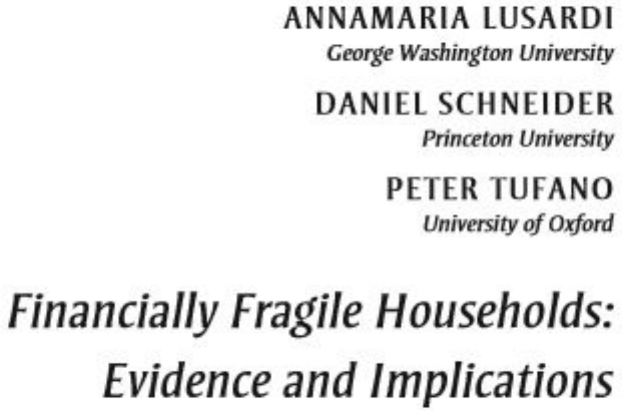


The Limits of Arbitrage

Andrei Shleifer; Robert W. Vishny

The Journal of Finance, Vol. 52, No. 1. (Mar., 1997), pp. 35-55.

Stable URL:
http://links.jstor.org/sici?sici=0022-1082%28199703%2952%3A1%3C35%3ATLOA%3E2.0.CO%3B2-3



ANNAMARIA LUSARDI
George Washington University

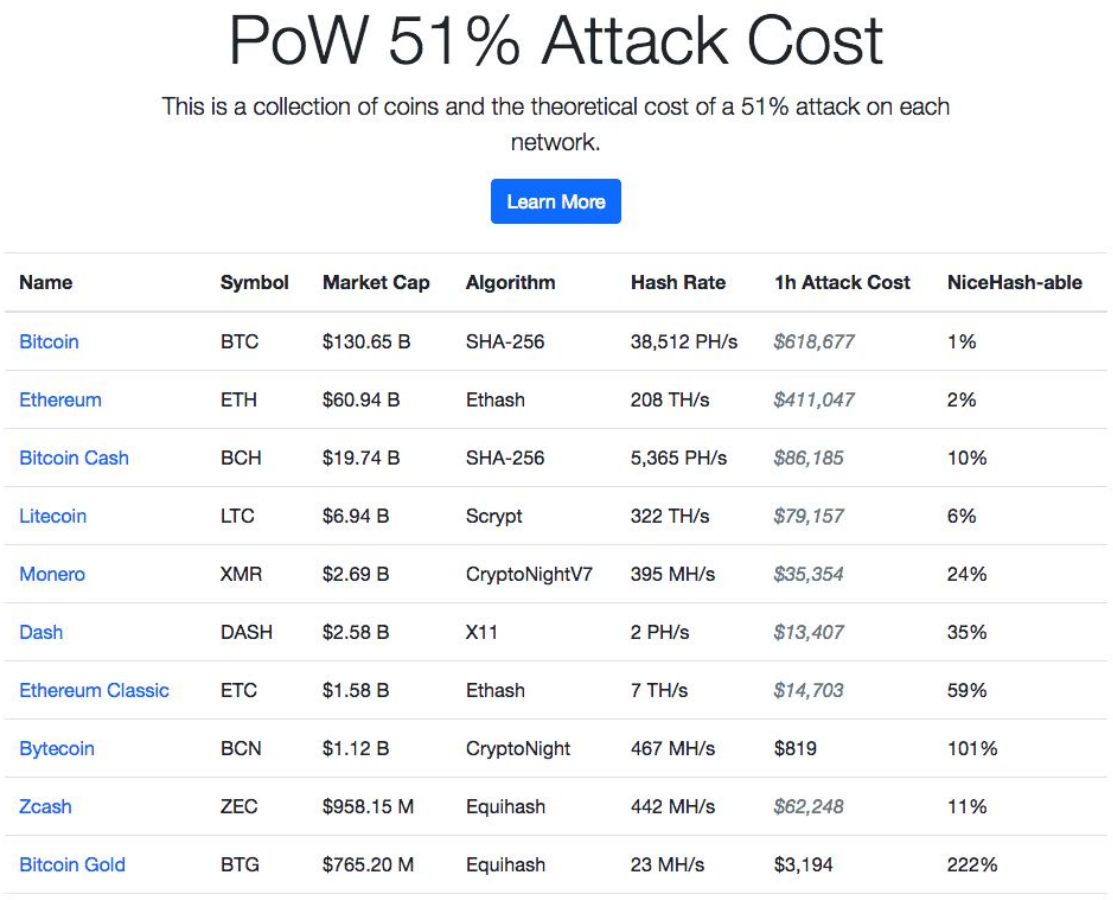
DANIEL SCHNEIDER
Princeton University

PETER TUFANO
University of Oxford

Financially Fragile Households: Evidence and Implications

Incentive system and economic rationale

PoW chain security depends on the “51% attack cost threshold”:



PoW 51% Attack Cost

This is a collection of coins and the theoretical cost of a 51% attack on each network.

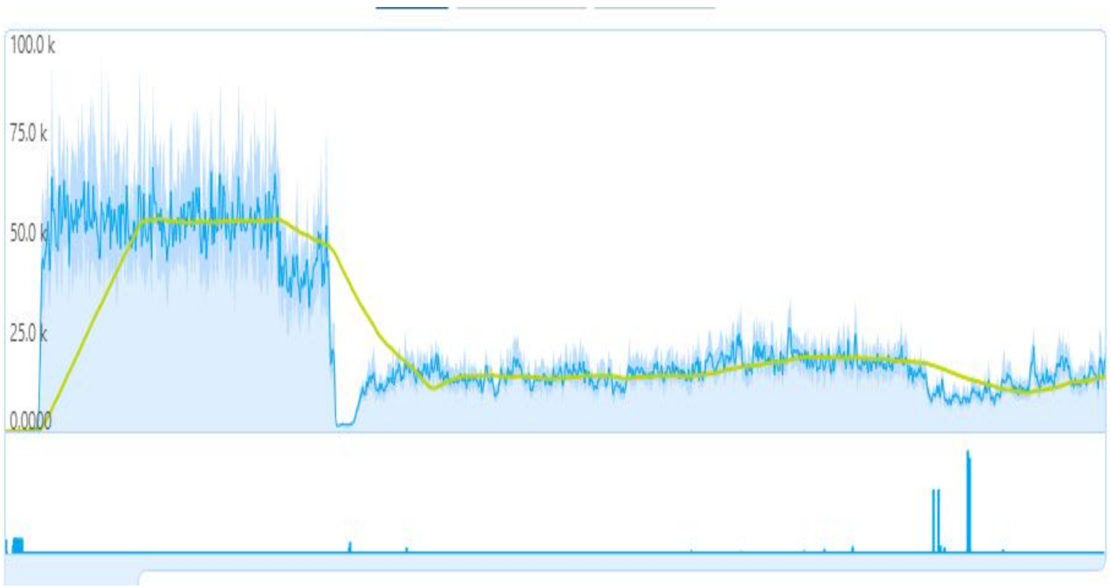
Name	Symbol	Market Cap	Algorithm	Hash Rate	1h Attack Cost	NiceHash-able
Bitcoin	BTC	$130.65 B	SHA-256	38,512 PH/s	*$618,677*	1%
Ethereum	ETH	$60.94 B	Ethash	208 TH/s	*$411,047*	2%
Bitcoin Cash	BCH	$19.74 B	SHA-256	5,365 PH/s	*$86,185*	10%
Litecoin	LTC	$6.94 B	Scrypt	322 TH/s	*$79,157*	6%
Monero	XMR	$2.69 B	CryptoNightV7	395 MH/s	*$35,354*	24%
Dash	DASH	$2.58 B	X11	2 PH/s	*$13,407*	35%
Ethereum Classic	ETC	$1.58 B	Ethash	7 TH/s	*$14,703*	59%
Bytecoin	BCN	$1.12 B	CryptoNight	467 MH/s	$819	101%
Zcash	ZEC	$958.15 M	Equihash	442 MH/s	*$62,248*	11%
Bitcoin Gold	BTG	$765.20 M	Equihash	23 MH/s	$3,194	222%

Incentive system and economic rationale

Normalizing supply fluctuation decreases poor decision-making:

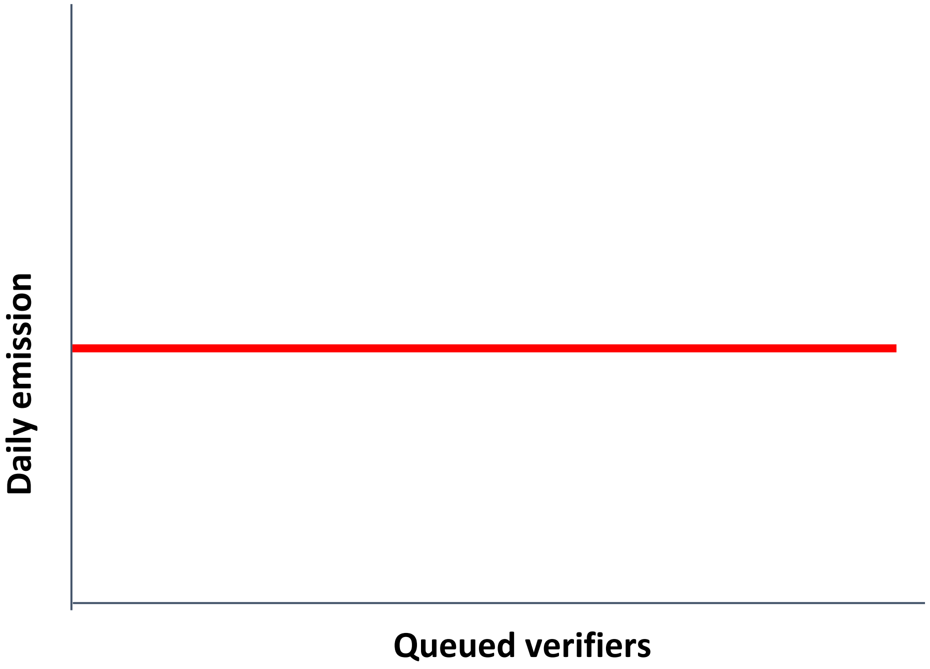
E = emission

W = work



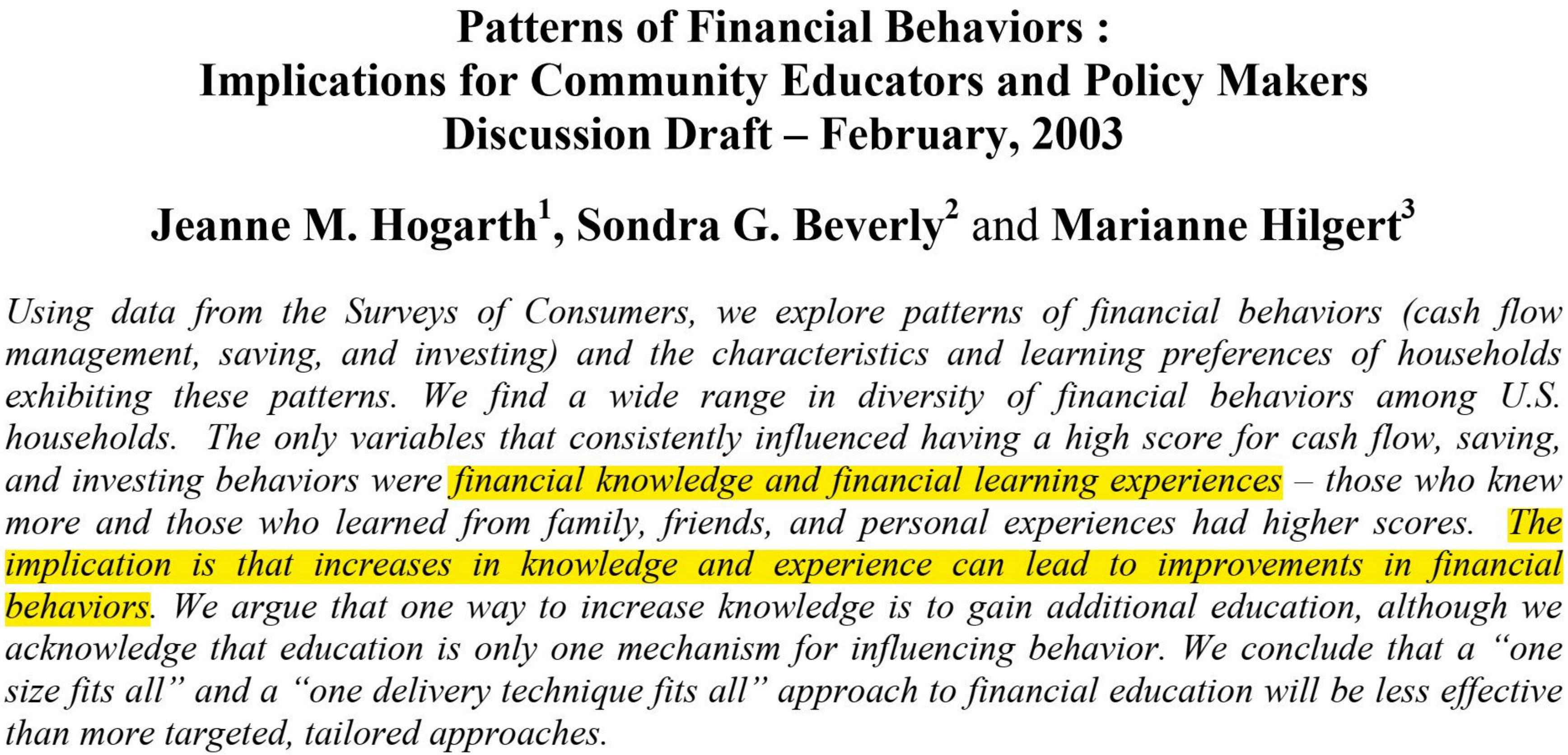
$$\frac{dE}{dW}! = 0$$

(large short-term variance, subject to retargeting)



$$\frac{dE}{dW} = 0$$

Incentive system and economic rationale



Patterns of Financial Behaviors :
Implications for Community Educators and Policy Makers
Discussion Draft – February, 2003

Jeanne M. Hogarth[1], **Sondra G. Beverly**[2] and **Marianne Hilgert**[3]

Using data from the Surveys of Consumers, we explore patterns of financial behaviors (cash flow management, saving, and investing) and the characteristics and learning preferences of households exhibiting these patterns. We find a wide range in diversity of financial behaviors among U.S. households. The only variables that consistently influenced having a high score for cash flow, saving, and investing behaviors were financial knowledge and financial learning experiences – those who knew more and those who learned from family, friends, and personal experiences had higher scores. The implication is that increases in knowledge and experience can lead to improvements in financial behaviors. We argue that one way to increase knowledge is to gain additional education, although we acknowledge that education is only one mechanism for influencing behavior. We conclude that a "one size fits all" and a "one delivery technique fits all" approach to financial education will be less effective than more targeted, tailored approaches.

TL;DR: never stop learning!