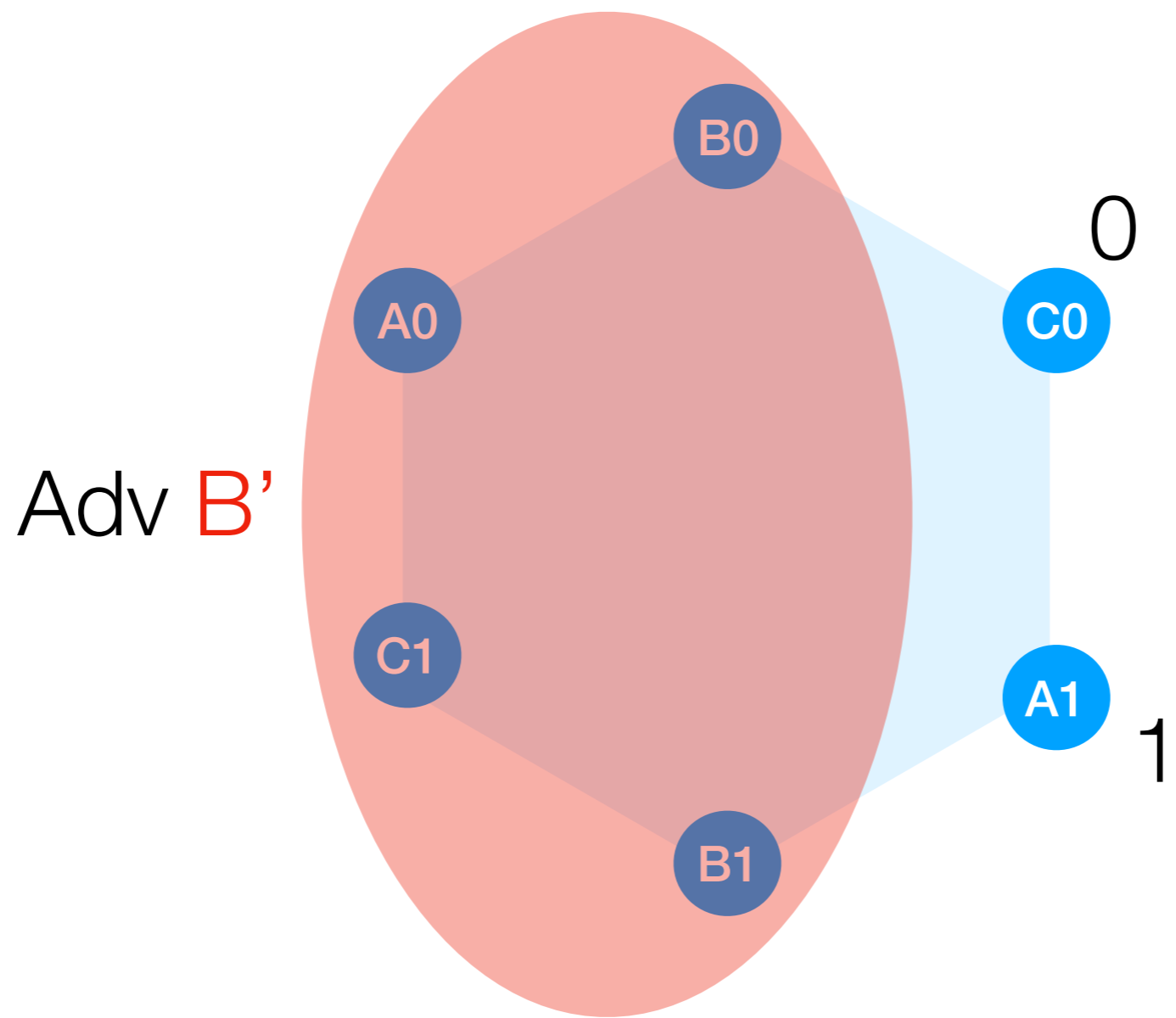


L11

Why does it work?

abhi shelat

Given PLS/FLM
impossibility, how can
Bitcoin tolerate $1/2$
adversary?



New adv model

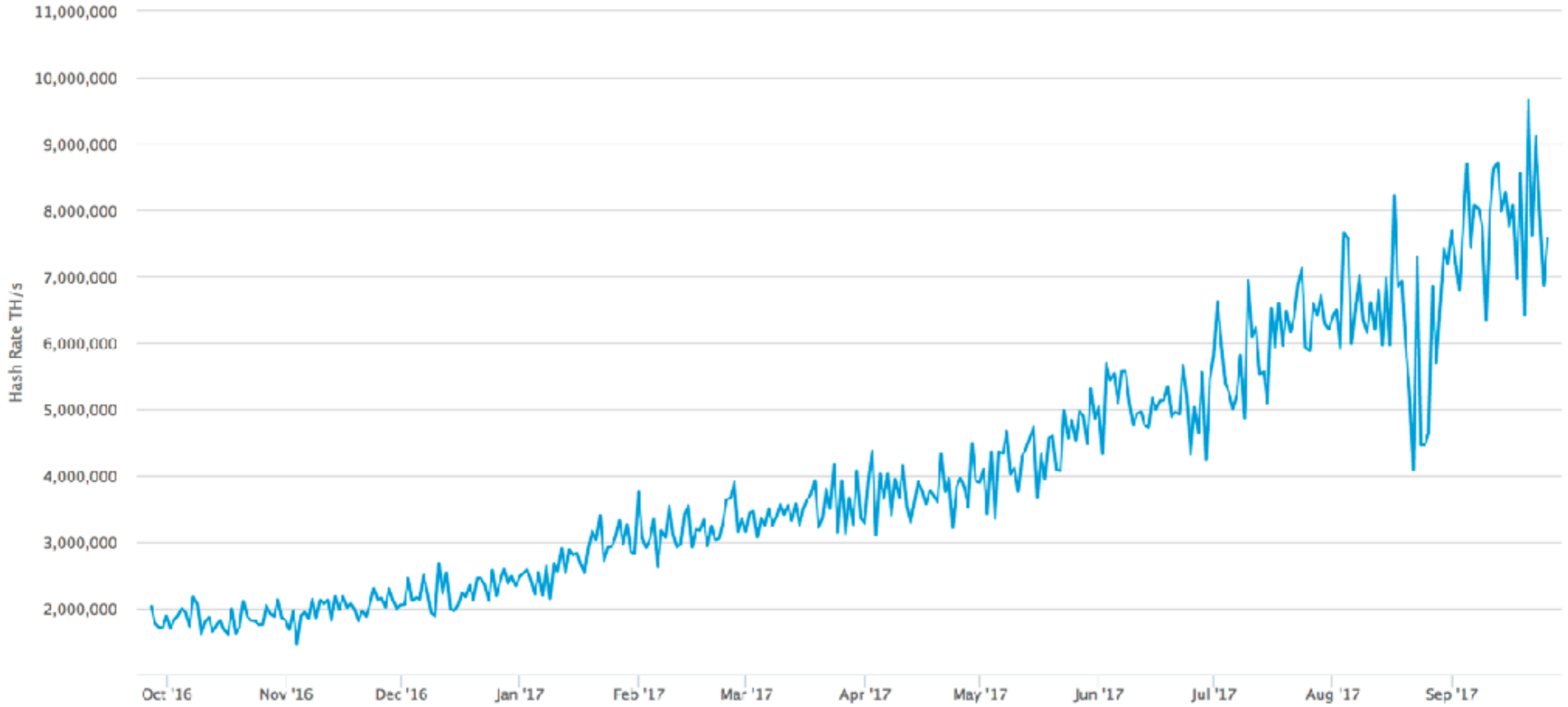
Adv controls $< 1/2$ of CPUs

How realistic is this model?

Hash Rate

The estimated number of tera hashes per second (trillions of hashes per second) the Bitcoin network is performing.

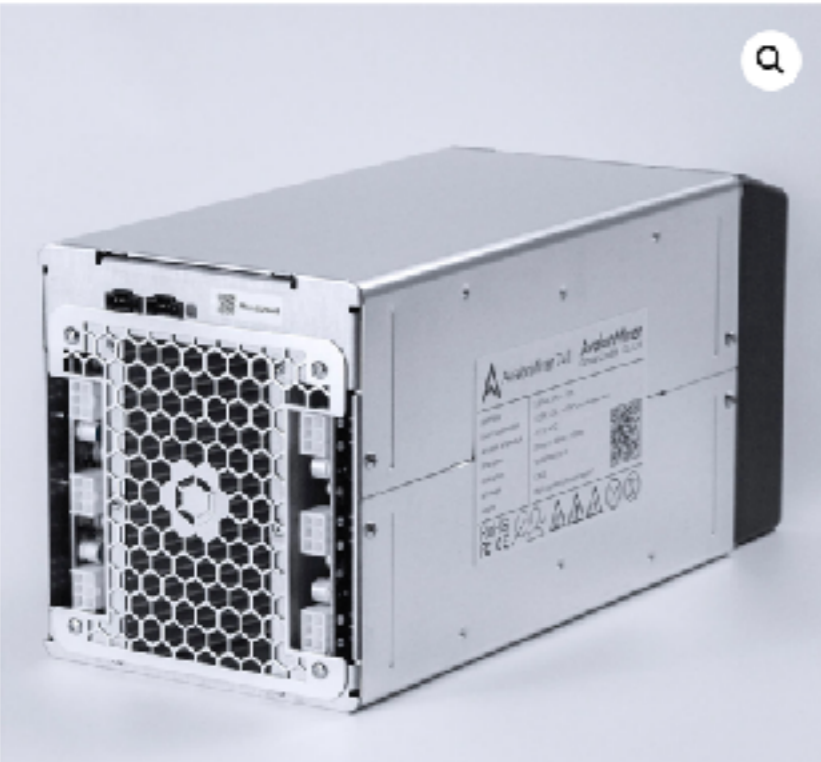
Source: blockchain.info



From blockchain.info

8m TH/s

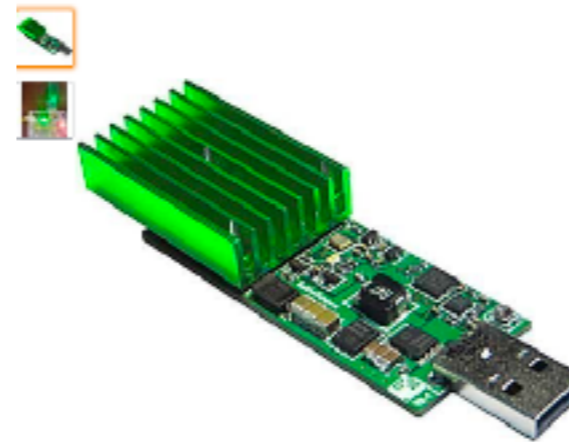
Home / AvalonMiner 741



AvalonMiner 741

\$798.00

Out of stock



GEKKOSCIENCE

GekkoScience Compac USB Stick Bitcoin Miner
8gh/s+ (BM1384)

★★★★☆ · 39 customer reviews | 50 answered questions

Note: This item is only available from third-party sellers (see all offers).

Available from these sellers.

- 15+gh/s mining speed(Higher speed requires usb port above spec)
- 31-35 watts per gh!
- Completely silent operation
- Bitcoin BM1384 chips
- See more product details

New (1) from \$69.97 + \$4.56 shipping

[Report incorrect product information.](#)

7.3 TH/s (RTHS) (7.3-8 RTH/s in field)

≈ 1150W, +0% ~ +15% (with 93% PSU efficiency @ 25 C)

0.16 Joules/GigaHash at the wall

Max 12.53

88 x A3212 16nm ASIC

Ethereum Network HashRate Growth Chart

Reset zoom



Source: Etherscan.io
Click and drag in the plot area to zoom in



Incentives

Not clear how to use a 51%
attack to earn back the
investment in mining hardware.

Why does it work?

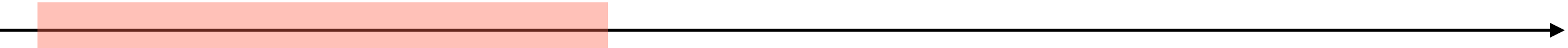
“Because it is hard to mine”



How to mine

1. Listen for new {blocks, txs}
2. Organize *valid* txs into a new pre-block
3. Hash pre-block, while changing nonce/
time/txs in pre-block in order to find a
valid block
4. Broadcast new valid blocks to peers.

Why does it work?



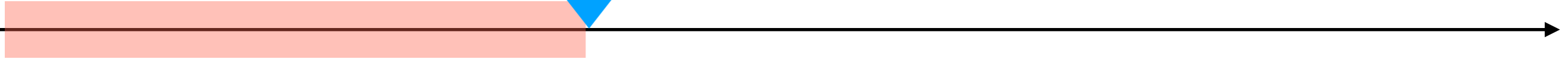
Period when nobody succeeds in mining. Everyone has same blockchain with **block A** at the top.

Why does it work?

Eureka! BOB finds a block **B** & broadcasts it.



Period when nobody succeeds in mining. Everyone has same blockchain with **block A** at the top.



Why does it work?

Eureka! BOB finds a block **B** & broadcasts it.



Period when nobody succeeds in mining. Everyone has same blockchain with **block A** at the top.

Block **B** is being transmitted over the network to all other miners.

Why does it work?

Eureka! BOB finds a block **B** & broadcasts it.



Period when nobody succeeds in mining. Everyone has same blockchain with **block A** at the top.

Block **B** is being transmitted over the network to all other miners.



Network Delay

Why does it work?

Eureka! BOB finds a block **B** & broadcasts it.



Period when nobody succeeds in mining. Everyone has same blockchain with **block A** at the top.

Block **B** is being transmitted over the network to all other miners.



All miners have received **B**. They now begin mining using **B** as the previous block.



Network Delay

What could go wrong?

Eureka! BOB finds a block **B** & broadcasts it.

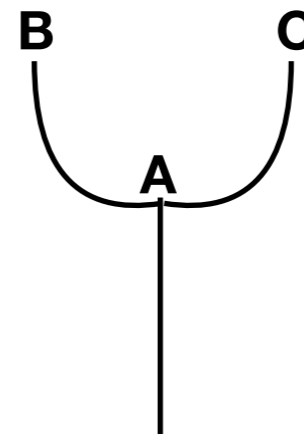
Eureka! ALICE finds a block **C** & broadcasts it.

Block **C** is being transmitted over the network.

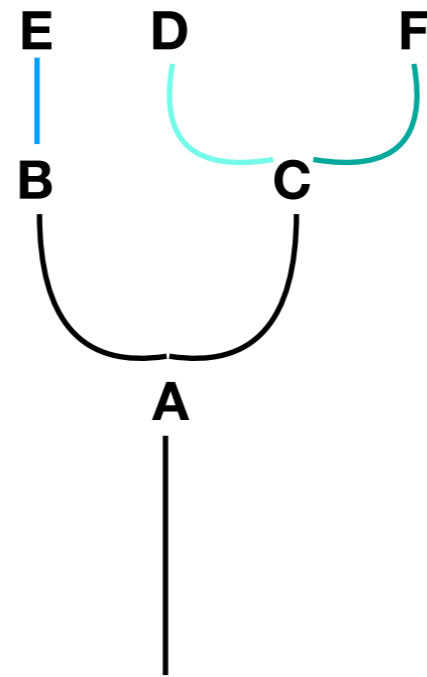
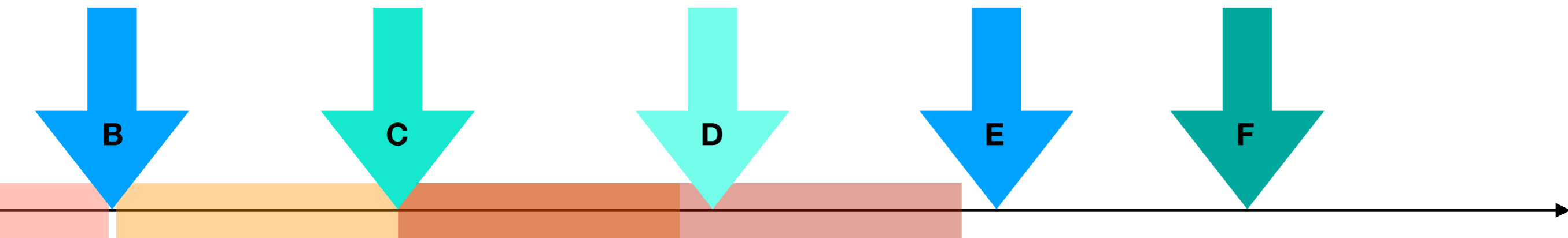
Period when nobody succeeds in mining. Everyone has same blockchain with **block A** at the top.

Block **B** is being transmitted over the network to all other miners.

Some miners received **B** first, some received **C** first. Network is trying to extend both **B** and **C**.

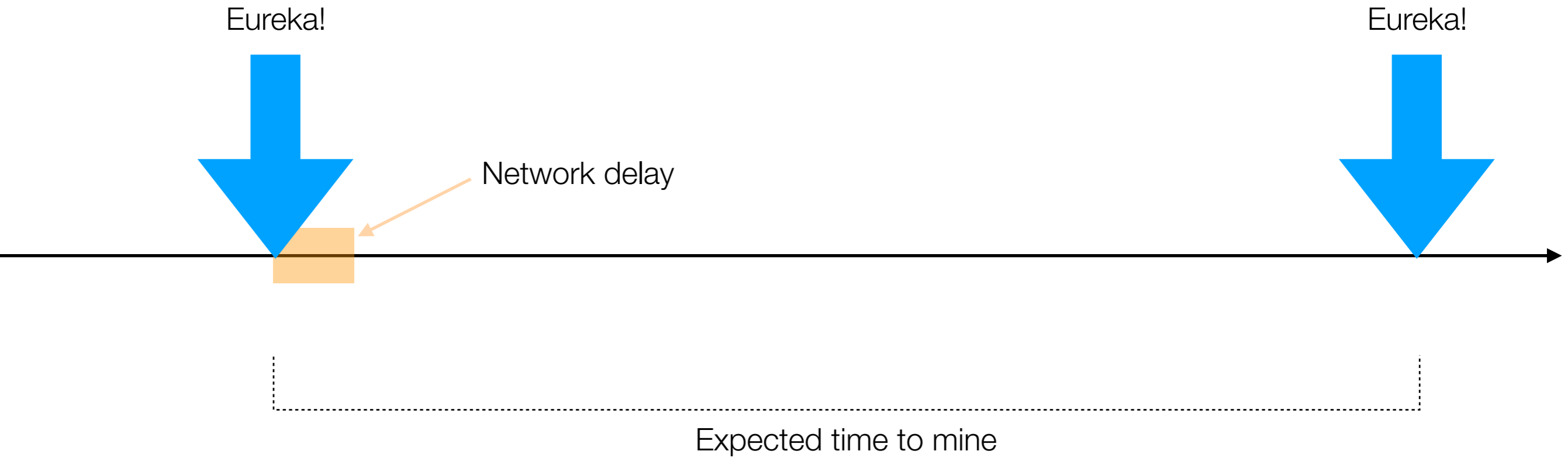


It could happen again



What prevents forking ad nauseum?

Network delay vs mining hardness



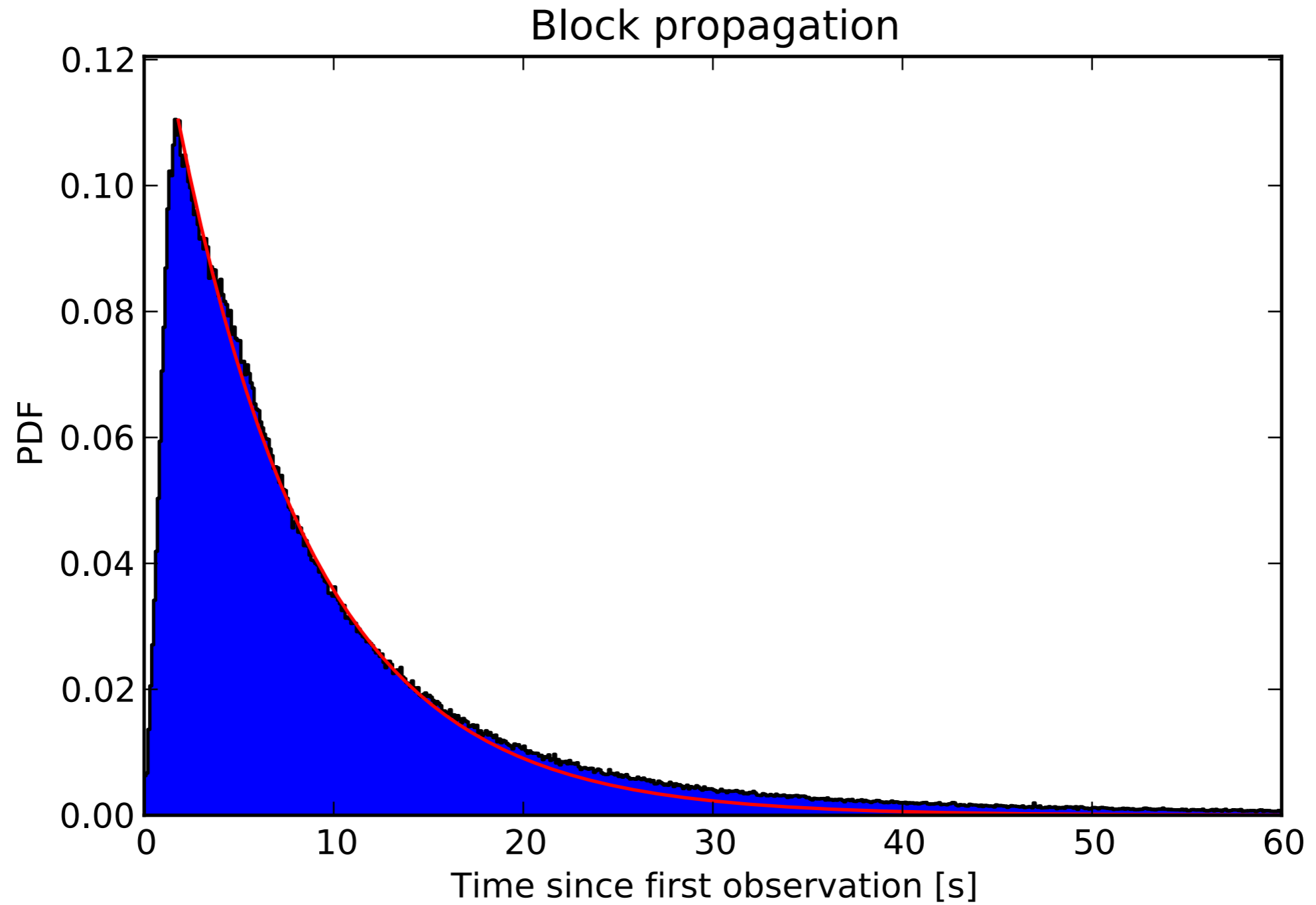


Fig. 3. The normalized histogram of times since the first block announcement with fitted exponential curve.

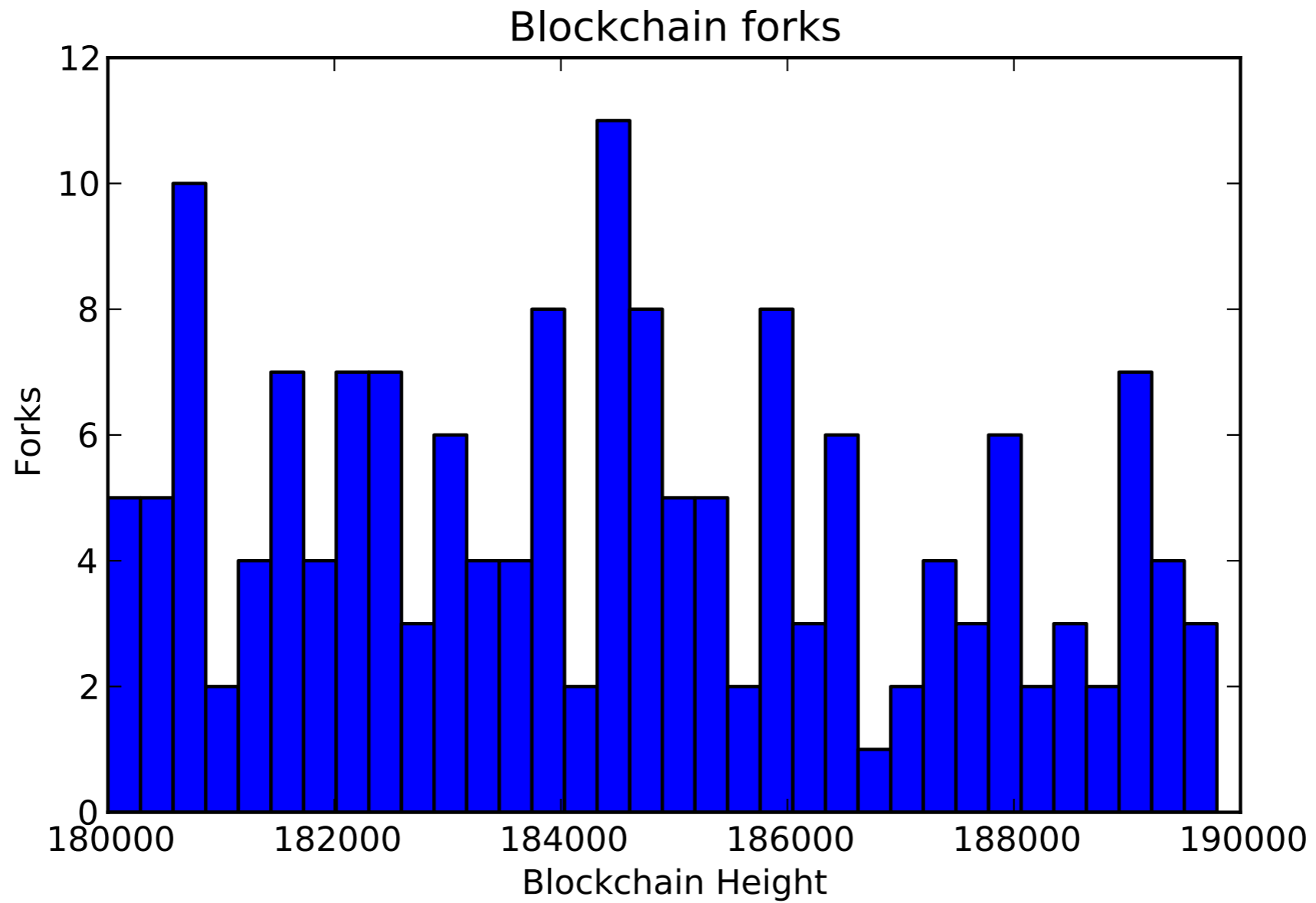


Fig. 5. Histogram of blockchain forks for 10'000 blocks starting at height 180'000, observed while participating in the network.

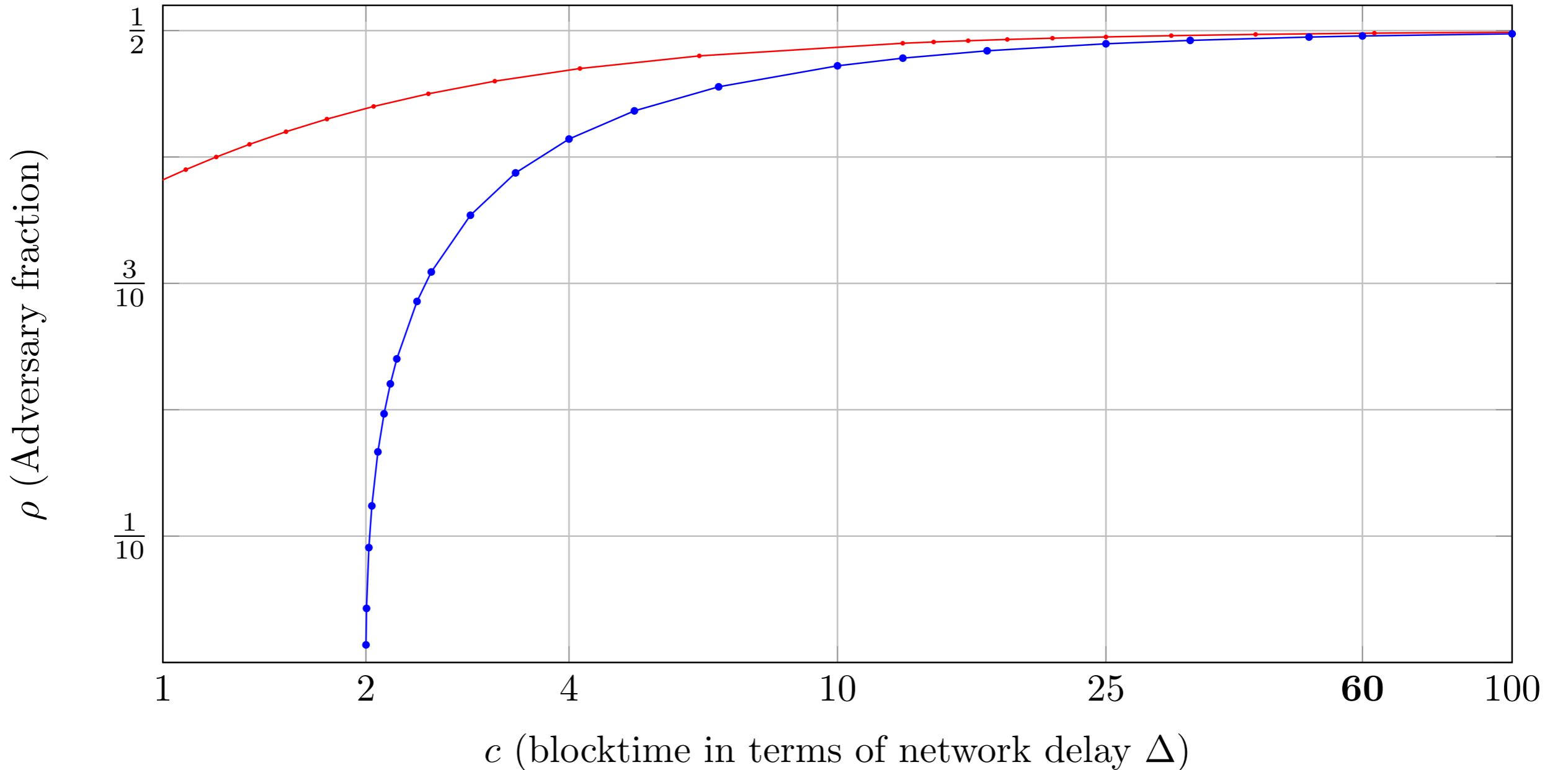
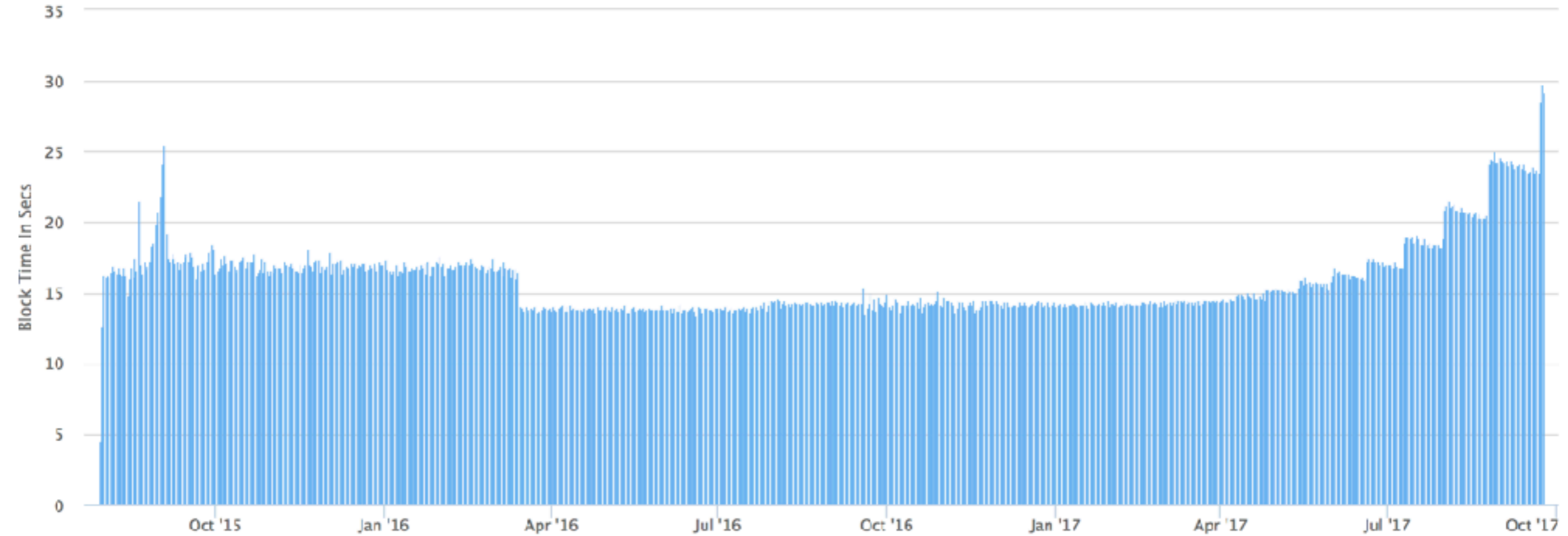













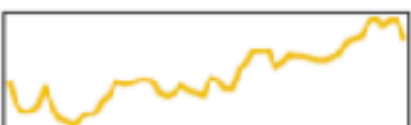



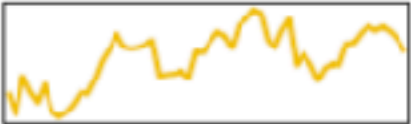






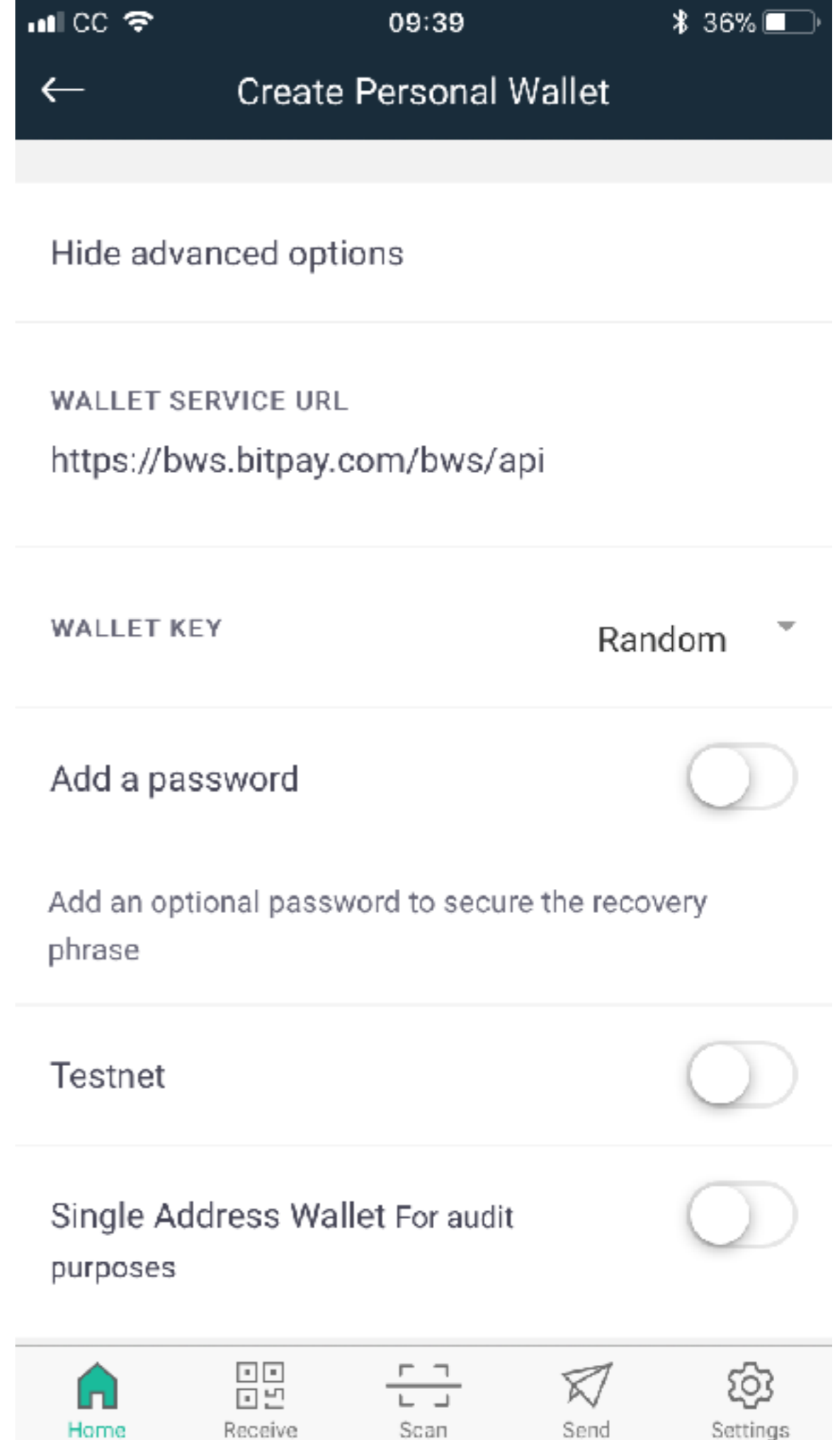
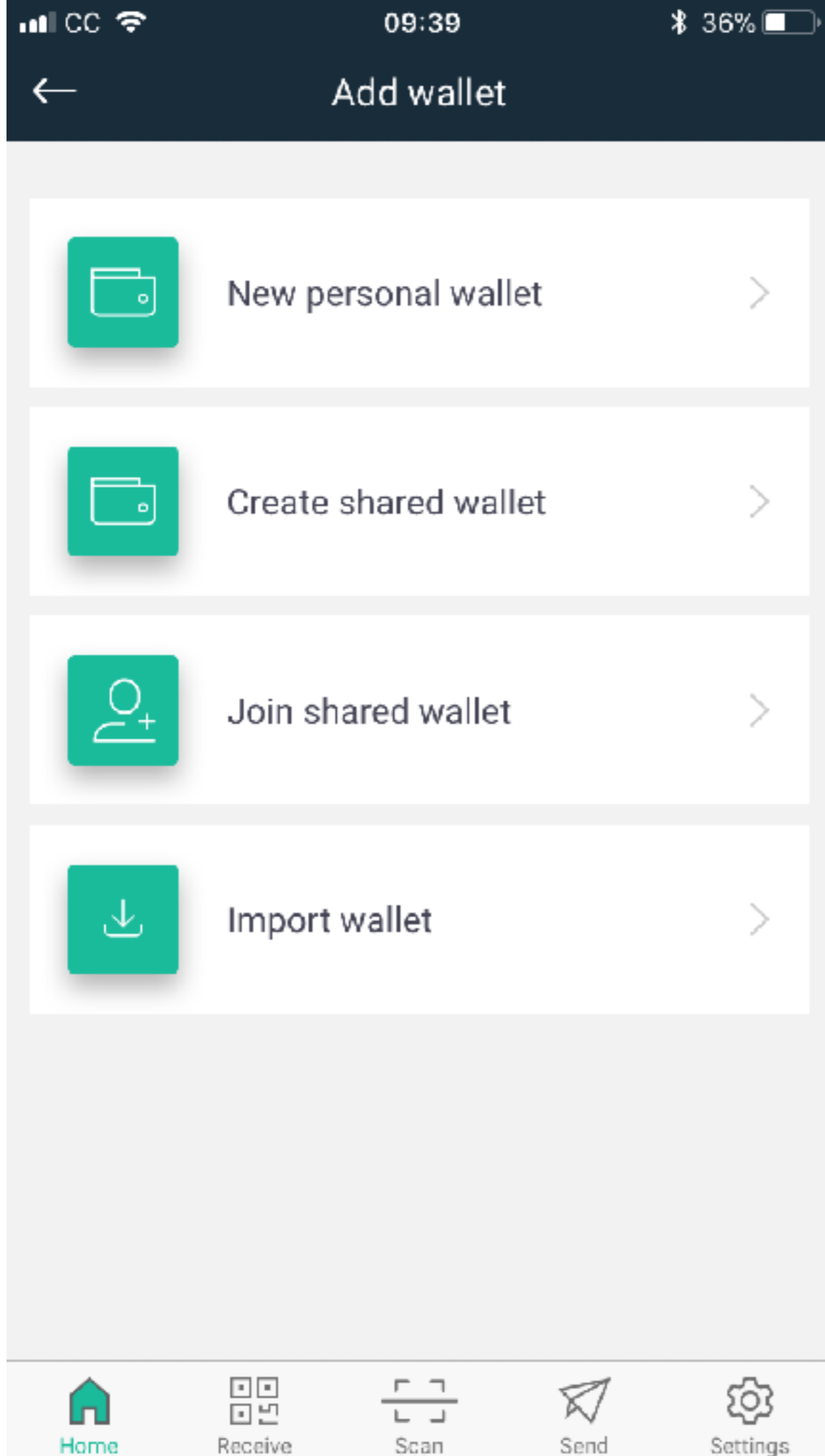
Figure 1: For $n = 10^5$ and $\Delta = 10^{13}$ (i.e., 10s delays at 1TH/s for commercially available mining hardware—these parameters roughly coincide with estimates of hashrate as of February 2016), we set hardness parameter $p = \frac{1}{c \cdot n \Delta}$ where c varies along the x -axis. We can interpret c as the expected blocktime in terms of the network delay Δ . The blue graph depicts a numerically-computed maximum value of ρ for which $\alpha(1 - (2\Delta + 2)\alpha) > \beta$, i.e. parameters under which our theorem shows consistency of the Nakamoto protocol. The gray plot shows our consistency theorem if Nakamoto adopted a deterministic tie-breaking rule. The red plot shows when our best attack succeeds in violating consistency. When $c = 60$,

Ethereum

Click and drag in the plot area to zoom in



#	Name	Market Cap	Price	Circulating Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	 Bitcoin	\$69,388,887,436	\$4182.11	16,591,837 BTC	\$1,898,160,000	2.80%	
2	 Ethereum	\$28,317,127,820	\$298.52	94,857,759 ETH	\$639,499,000	1.54%	
3	 Ripple	\$7,451,818,919	\$0.194342	38,343,841,883 XRP *	\$175,863,000	-3.40%	
4	 Bitcoin Cash	\$7,371,829,648	\$443.45	16,623,775 BCH	\$245,437,000	-1.81%	
5	 Litecoin	\$2,883,557,824	\$54.27	53,134,432 LTC	\$247,311,000	1.20%	
6	 Dash	\$2,537,772,243	\$334.60	7,584,496 DASH	\$60,020,700	-2.44%	
7	 NEM	\$2,122,794,000	\$0.235866	8,999,999,999 XEM *	\$3,741,010	0.15%	
8	 NEO	\$1,485,055,000	\$29.70	50,000,000 NEO *	\$147,363,000	-7.00%	
9	 IOTA	\$1,478,893,560	\$0.532066	2,779,530,283 MIOTA *	\$10,741,900	-1.66%	
10	 Monero	\$1,461,394,112	\$96.49	15,145,001 XMR	\$58,145,300	-0.24%	
11	 Ethereum Classic	\$1,217,571,758	\$12.69	95,946,585 ETC	\$204,739,000	7.38%	



<https://github.com/ethereum/mist/releases>