Zcash Observatory

Gardening Club update (2020-05-05)

Pranav Thirunavukkarasu

Blockchain engineer at Insight

Mitchell Krawiec-Thayer

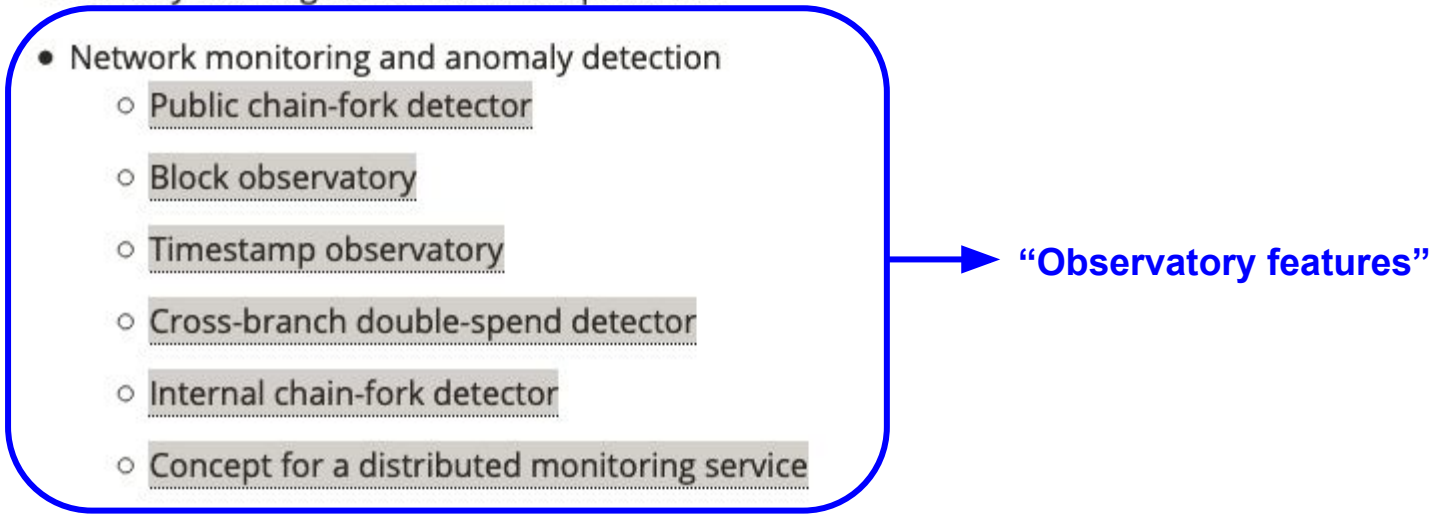
Head of Research at Insight

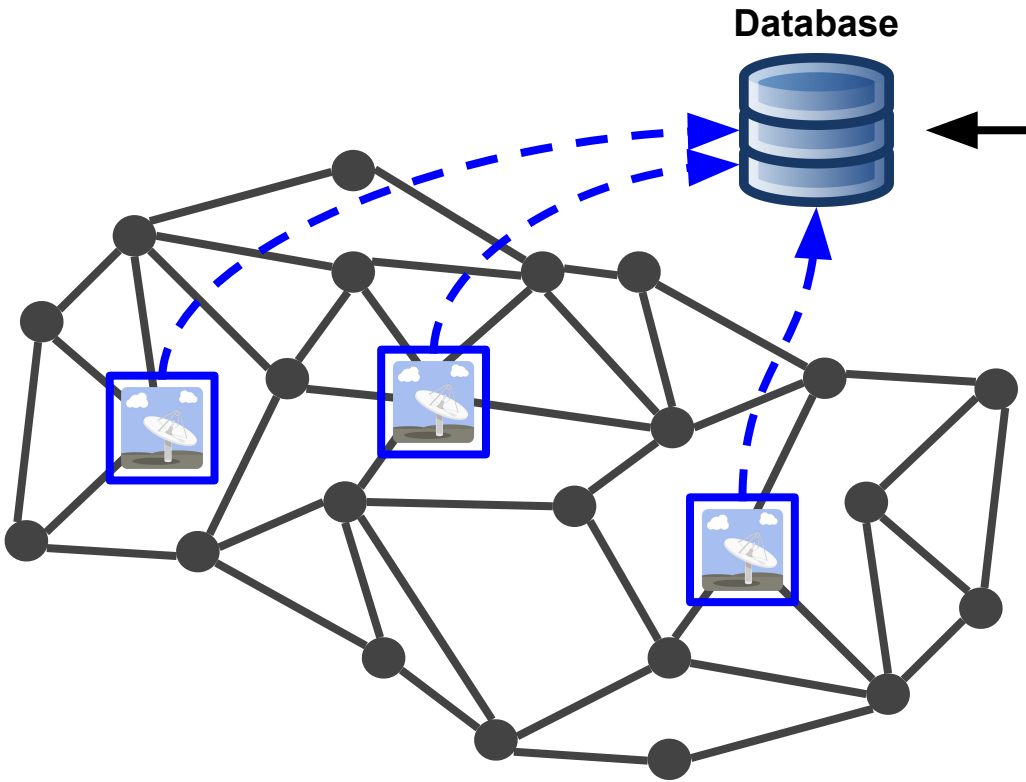
Core and Security

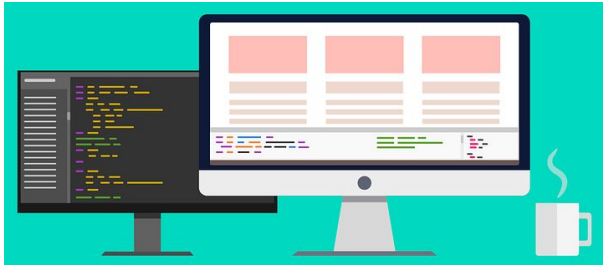
- Continued support for alternative implementations (such as Parity Zcash)
- Security auditing for the code and protocols
- Network monitoring and anomaly detection
  - Public chain-fork detector
  - Block observatory
  - Timestamp observatory
  - Cross-branch double-spend detector
  - Internal chain-fork detector
  - Concept for a distributed monitoring service
- Formal verification
  - Identify parts of the Zcash codebase that are security-critical and conducive to formal methods for proving correctness of code

Core and Security

- Continued support for alternative implementations (such as Parity Zcash)
- Security auditing for the code and protocols
- Network monitoring and anomaly detection
  - Public chain-fork detector
  - Block observatory
  - Timestamp observatory
  - Cross-branch double-spend detector
  - Internal chain-fork detector
  - Concept for a distributed monitoring service
- Formal verification
  - Identify parts of the Zcash codebase that are security-critical and conducive to formal methods for proving correctness of code





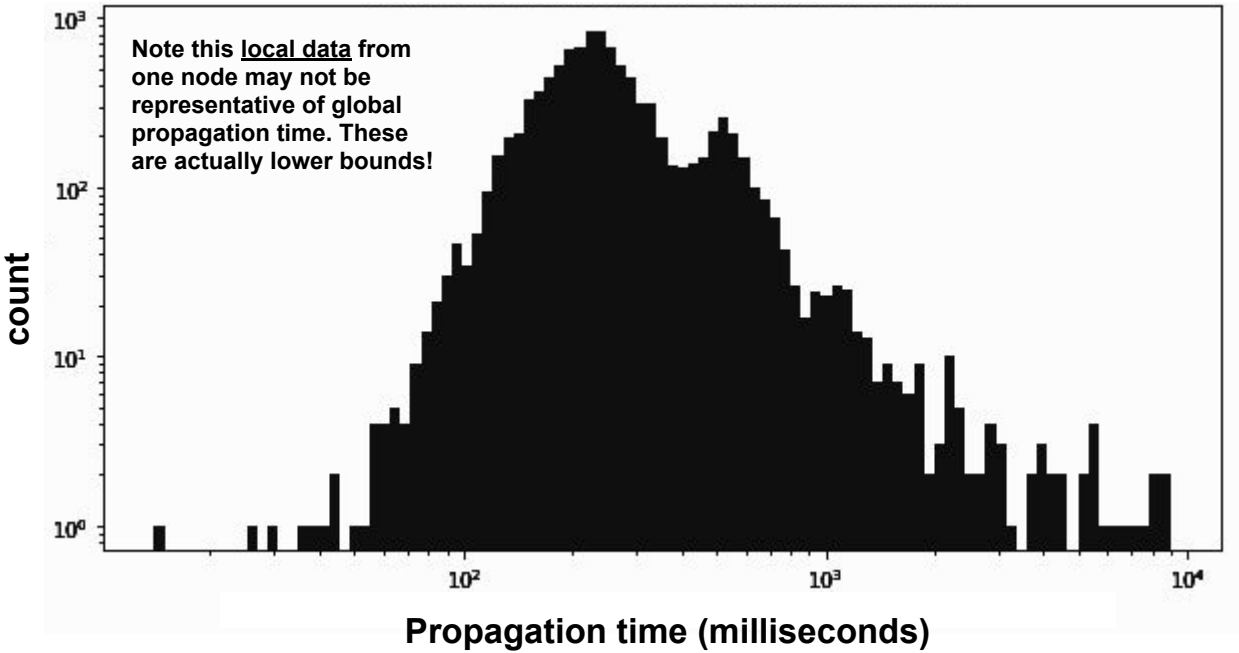


Dashboard, alerts, etc

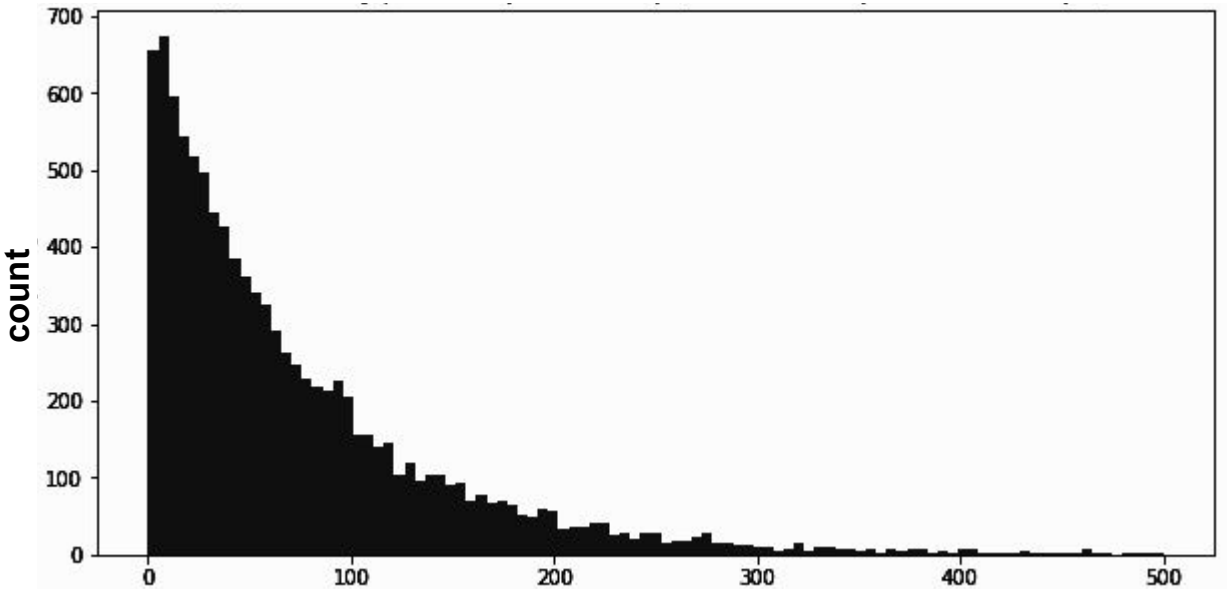
- Network Security
  - Alternative/stale blocks
  - Potential double spend attacks
  - Selfish/stubborn mining detection
- Network Performance
  - Block/txn propagation time
  - Network connectivity
  - Network centralization

Block propagation time

(heard from last peer) - (heard from first peer)

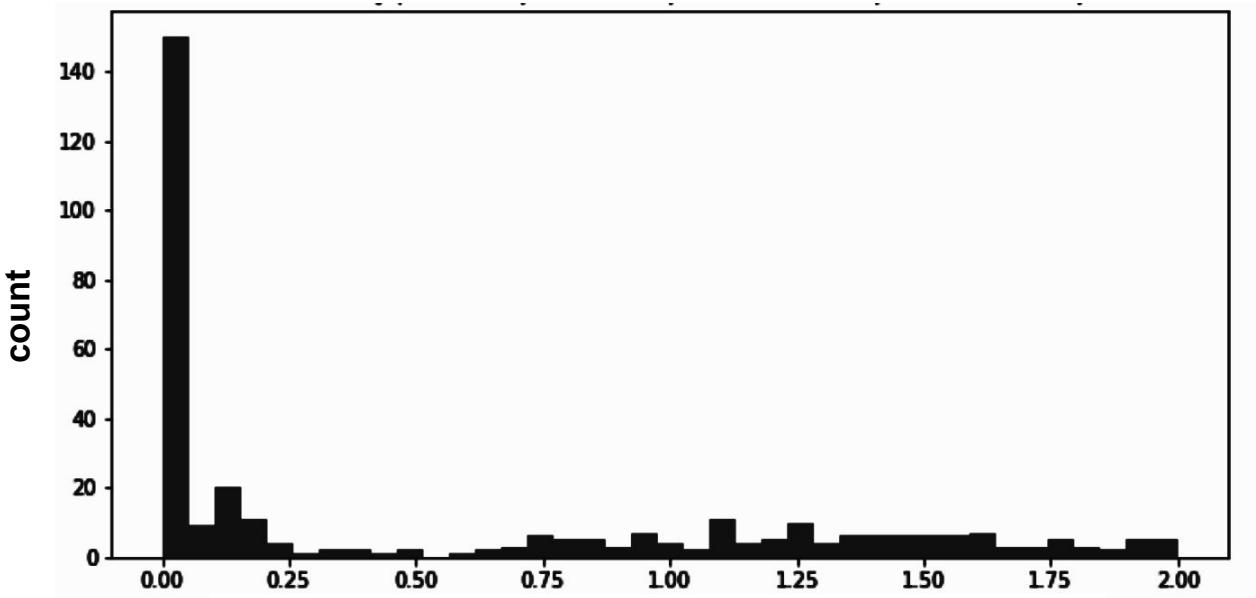


Real block interval



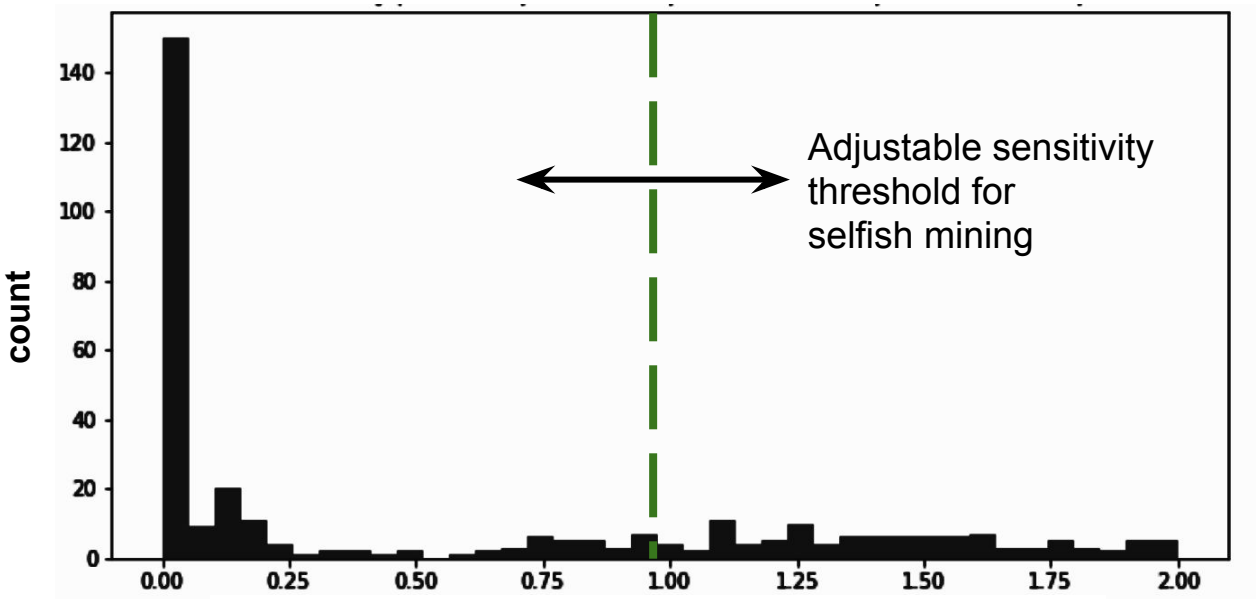
NOT based on miner timestamps

Real block interval



NOT based on miner timestamps

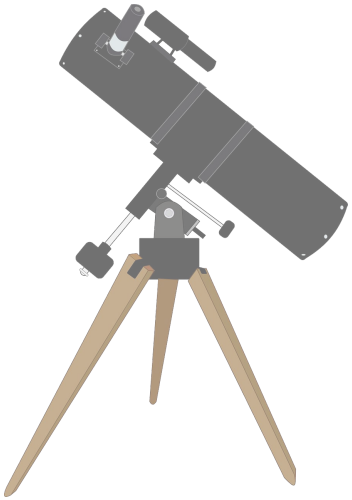
Real block interval



NOT based on miner timestamps

Status

Feature	Status	Funder
Advanced logging	Submitted PR to Zcash	Zcash Foundation
NetSec alerts	Prototyped	Zcash Foundation
Research pipelines	Prototyped	Zcash Foundation
Global network	Partially architected	TBD - you?
Dashboard / front-end	Design underway	TBD - you?



Shielded sponsorship

zs1gvj8aha3drjnerl3fxp3etwa2s8yepp45yqdk
ueuewe2cmuyadxyaxc838k5vcrldxdxv80atp6

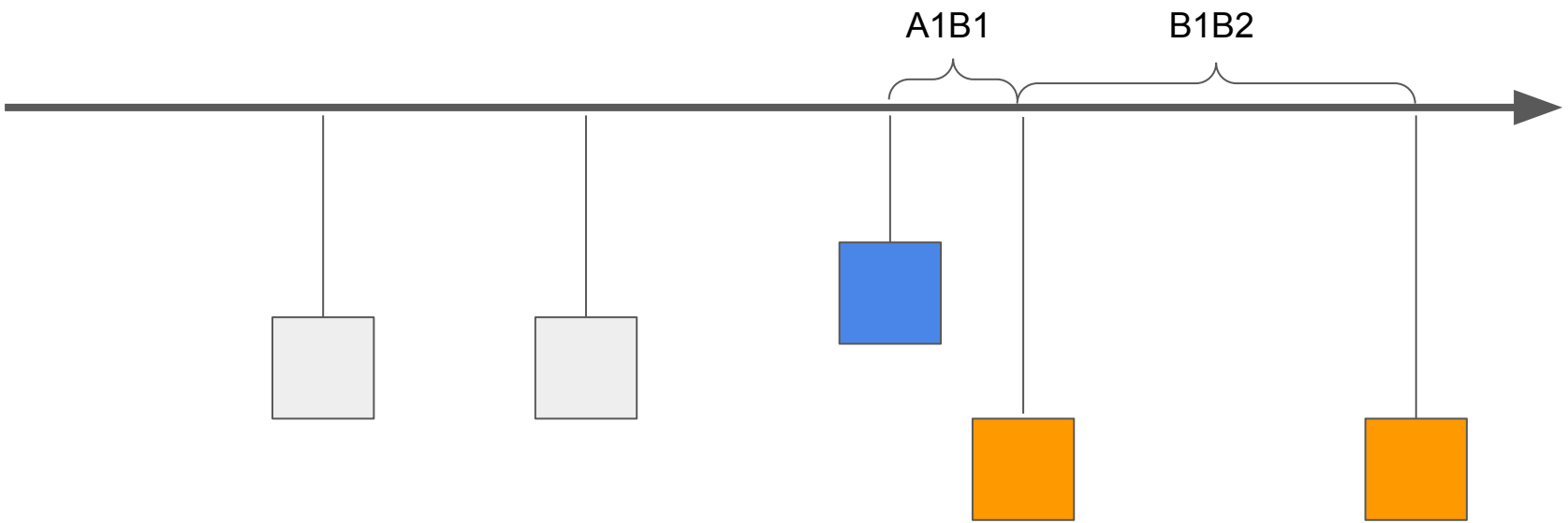
Transparent sponsorship

t1LWFw5i5La9WJ1SBfn4VZ74L2dkVHUzoB4

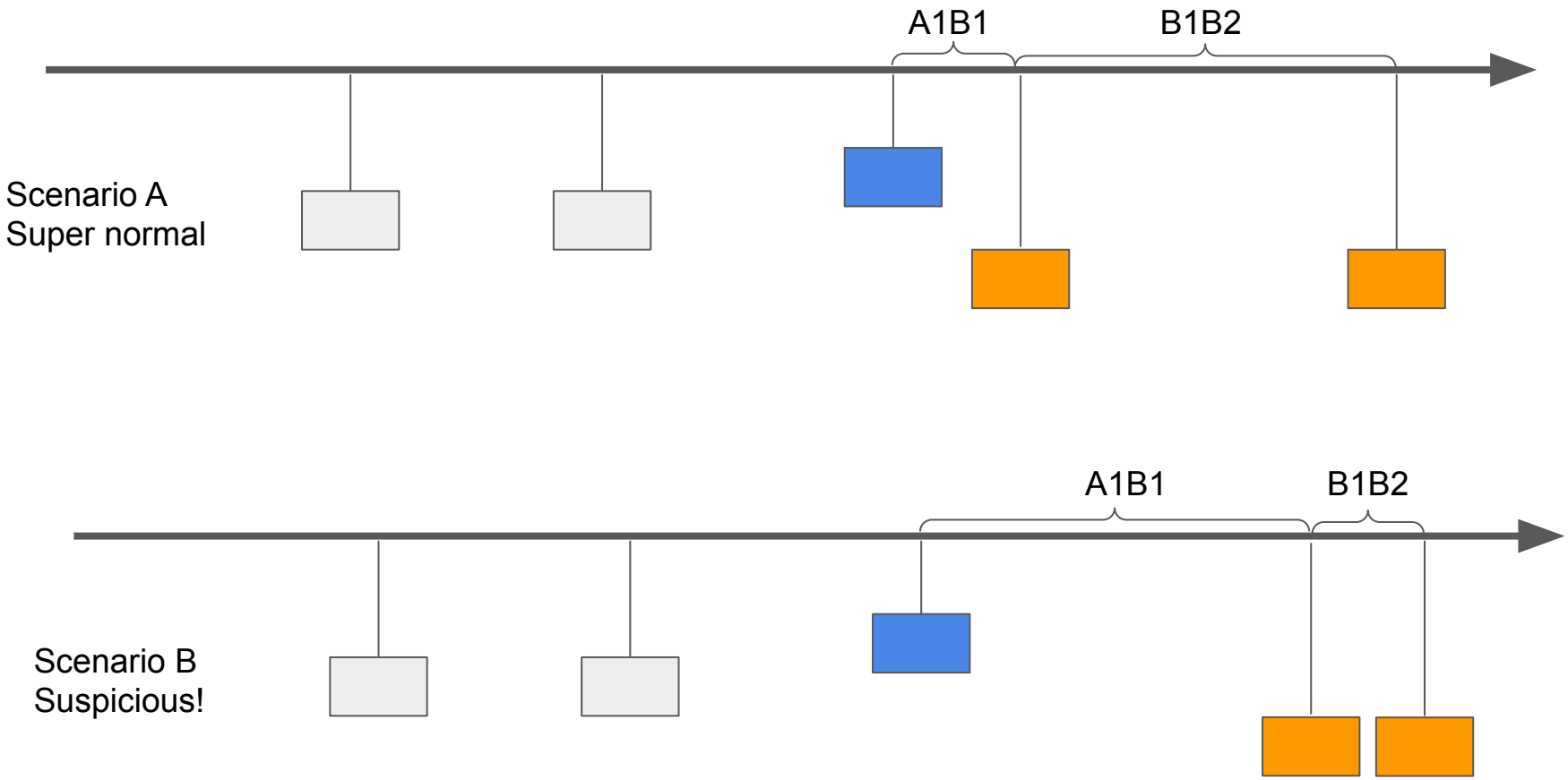
Want to learn more, or donate fiat to support Observatory R & D?
Visit fellows.link/ObservatoryDev or contact Mitchell@InsightFellows.com

Questions?

Supplemental



If A1B1 < 2*global_latency
    Not suspicious. Nothing to see here
If A1B1 >> global_latency
    Potentially interesting
If A1B1 > block_time & B1B2 is small
    VERY suspicious


A1B1
B1B2
Scenario A
Super normal
A1B1
B1B2
Scenario B
Suspicious!

Selfish mining “*detection algorithm A1B1*”

IF

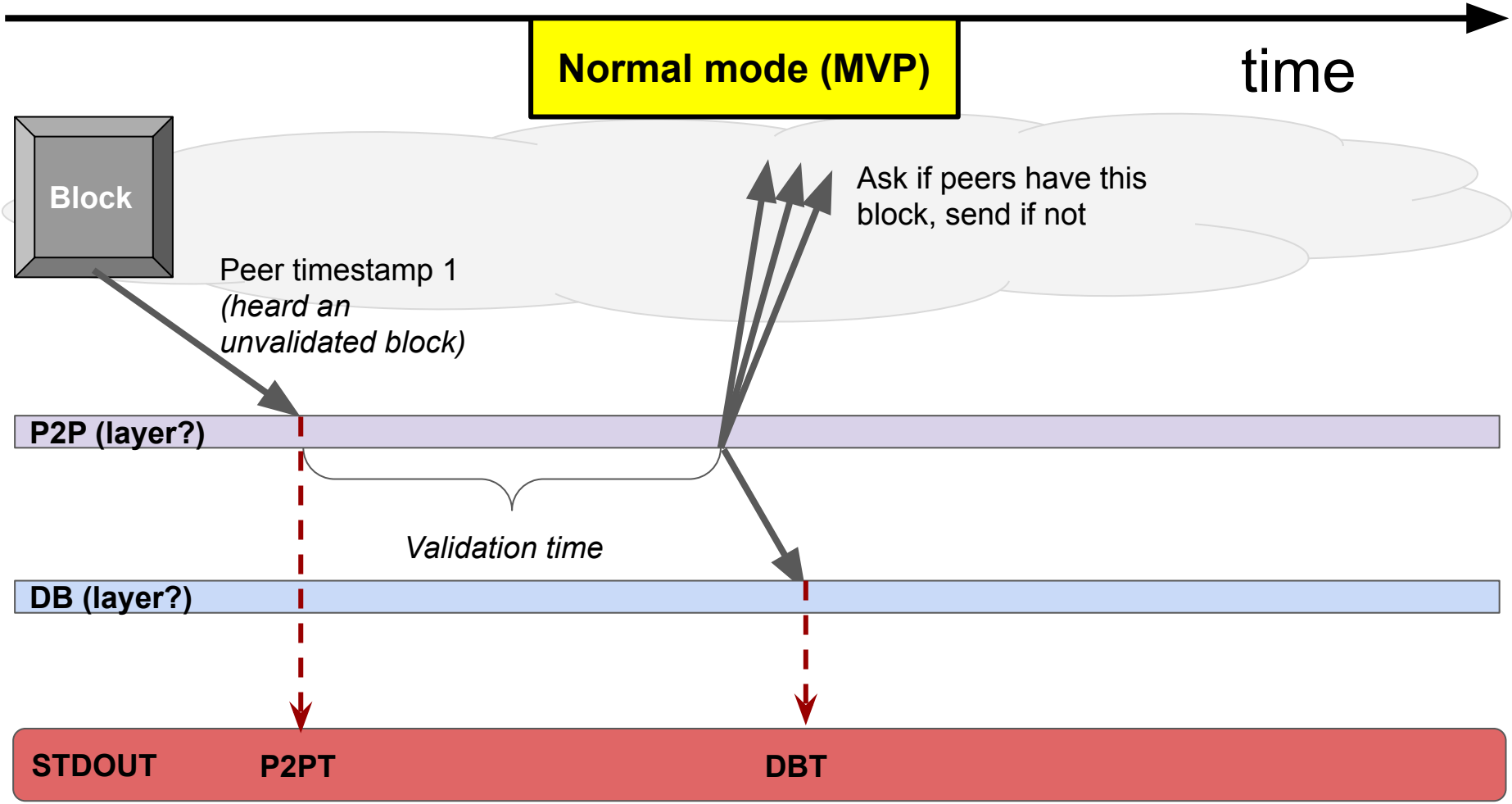
(1) there is a reorg

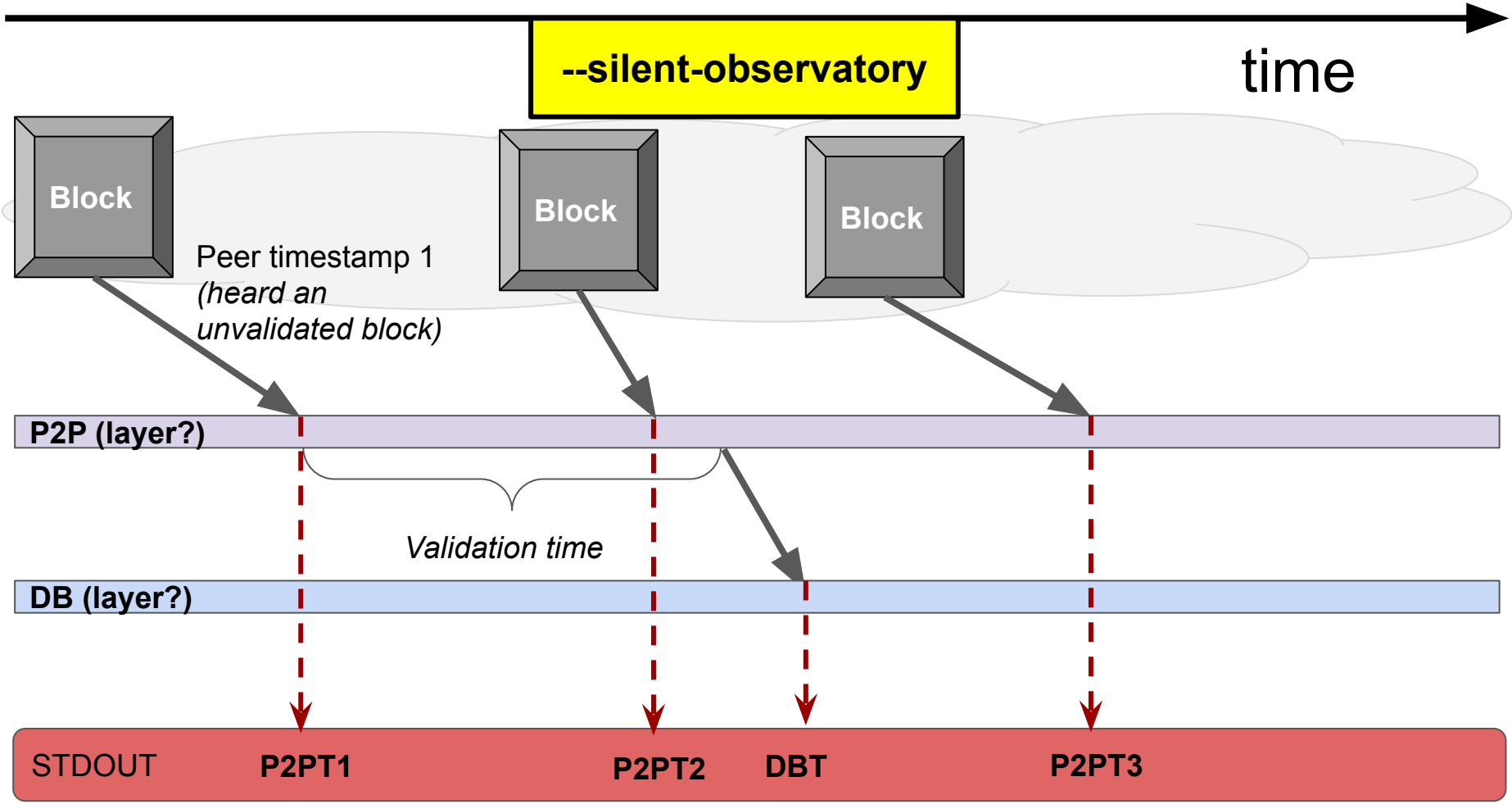
and

(2) A1B1 > k*global_latency

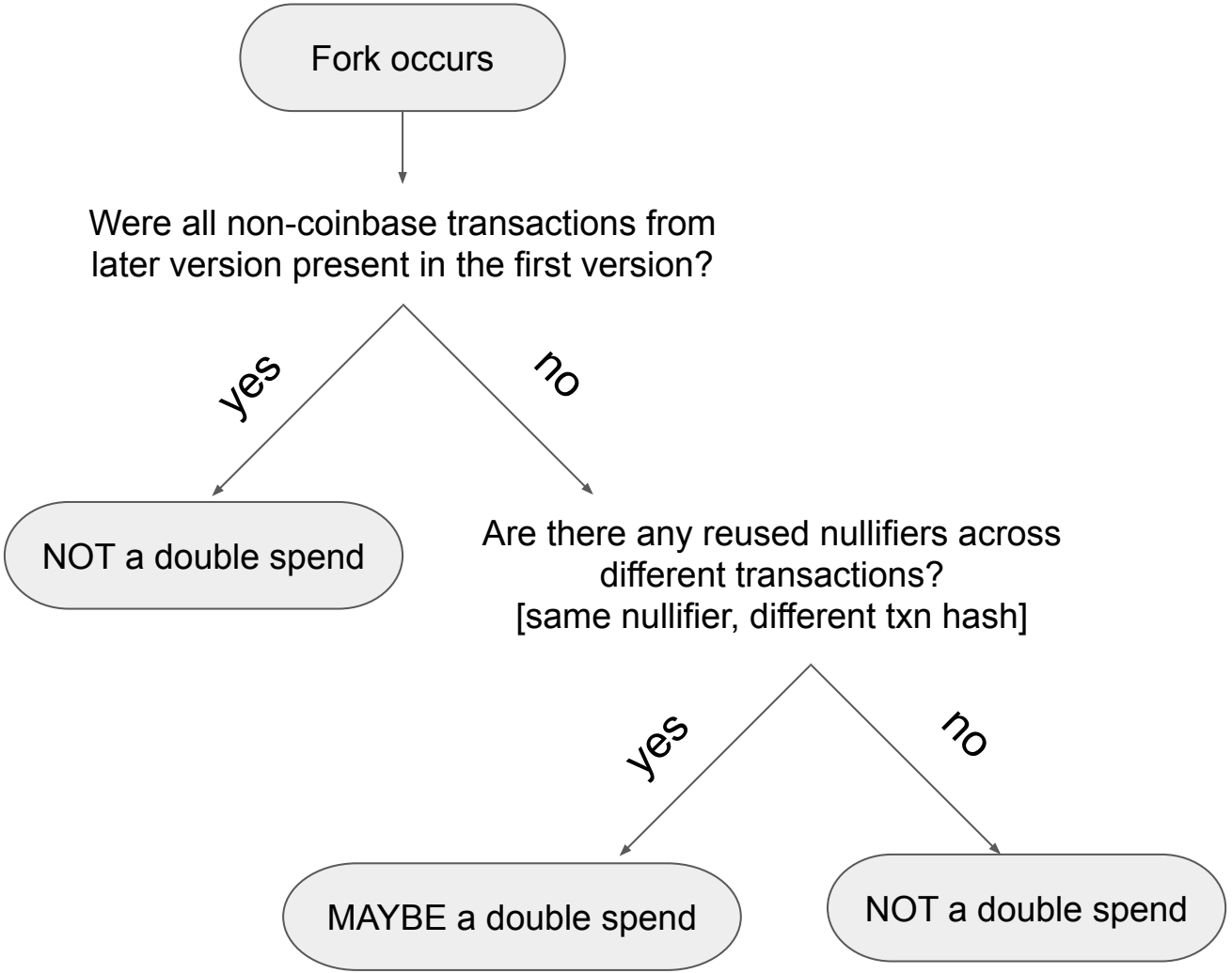
THEN throw a “possible selfish mining” flag

(let k = 3 by default)

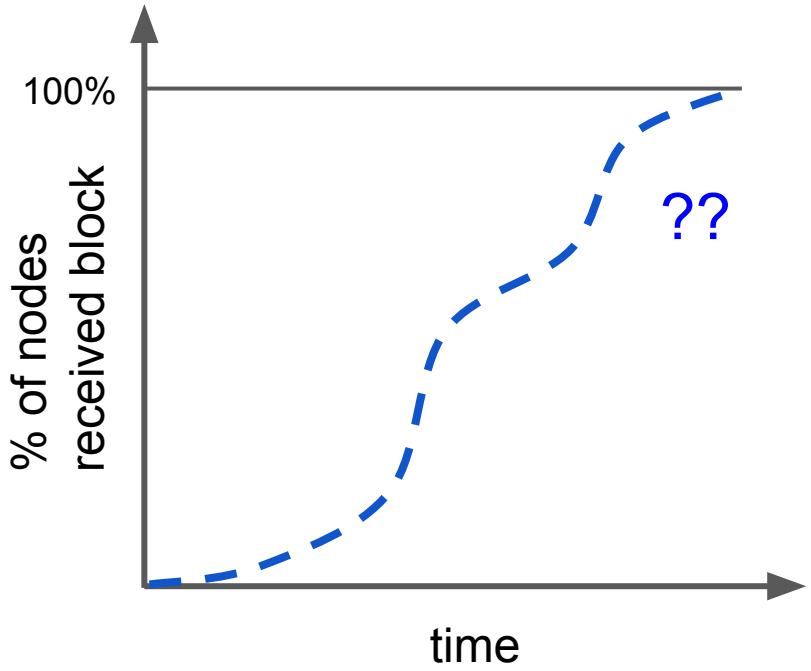

Normal mode (MVP)
time
Block
Peer timestamp 1
(heard an
unvalidated block)
Ask if peers have this
block, send if not
P2P (layer?)
Validation time
DB (layer?)
STDOUT
P2PT
DBT



^^ Note this edge case that P2PT2+ may come before validation is complete (DBT)

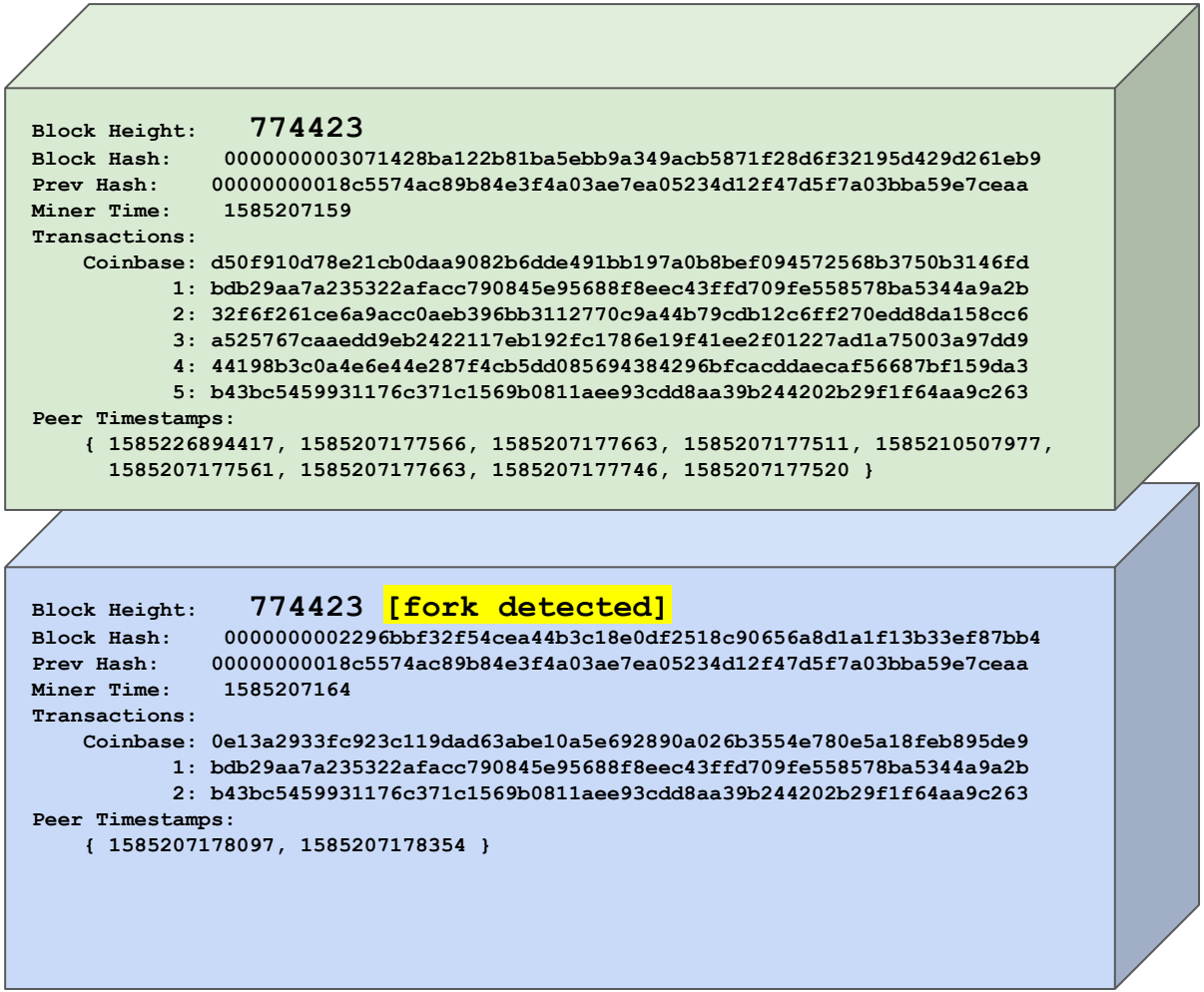

Fork occurs
Were all non-coinbase transactions from later version present in the first version?
yes
no
NOT a double spend
Are there any reused nullifiers across different transactions?
[same nullifier, different txn hash]
yes
no
MAYBE a double spend
NOT a double spend

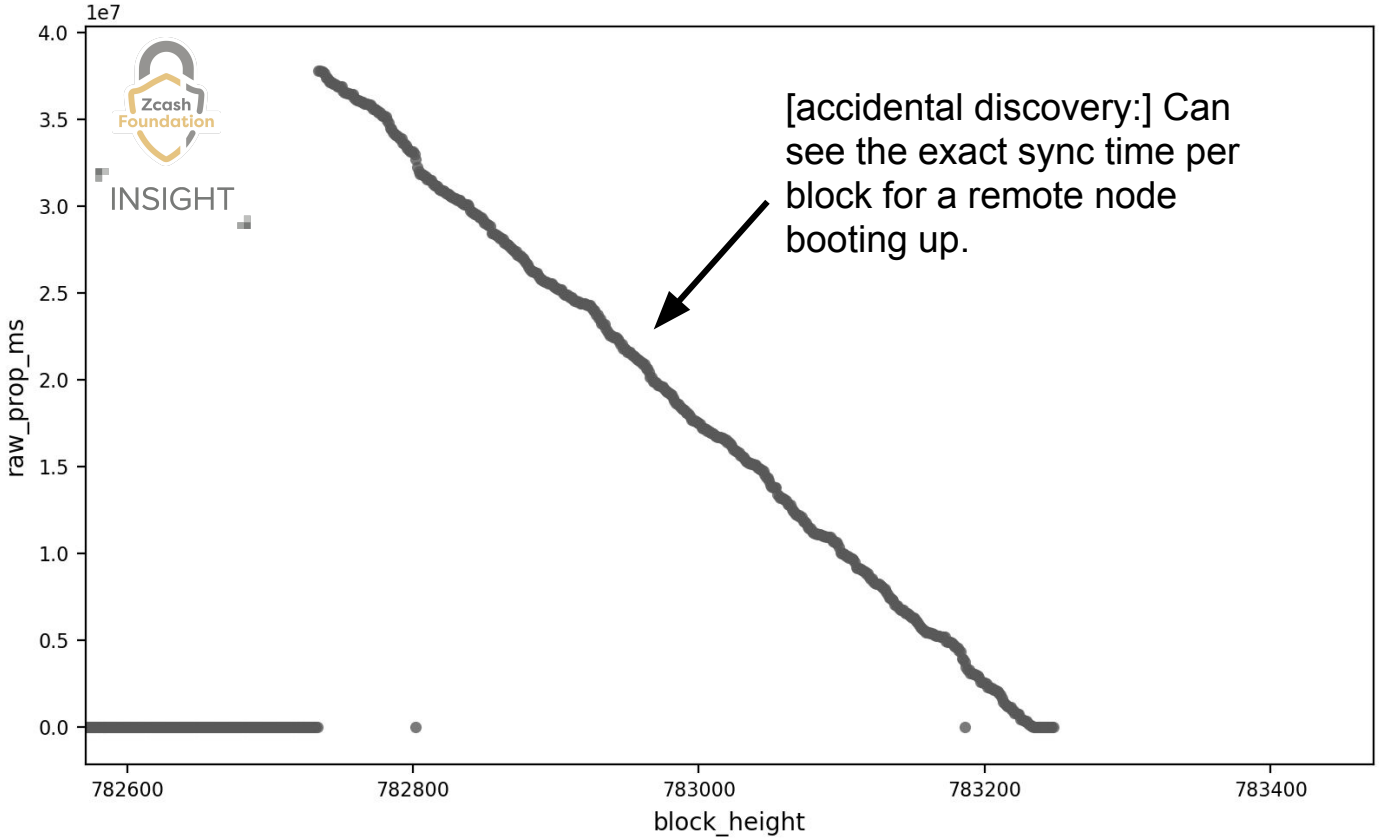
What is the shape of this curve in theory and practice?
Any good articles or data sources for this?



```
Block Height:    774423
Block Hash:    0000000003071428ba122b81ba5ebb9a349acb5871f28d6f32195d429d261eb9
Prev Hash:    00000000018c5574ac89b84e3f4a03ae7ea05234d12f47d5f7a03bba59e7ceaa
Miner Time:    1585207159
Transactions:
    0:    d50f910d78e21cb0daa9082b6dde491bb197a0b8bef094572568b3750b3146fd
    1:    bdb29aa7a235322afacc790845e95688f8eec43ffd709fe558578ba5344a9a2b
    2:    32f6f261ce6a9acc0aeb396bb3112770c9a44b79cdb12c6ff270edd8da158cc6
    3:    a525767caaedd9eb2422117eb192fc1786e19f41ee2f01227ad1a75003a97dd9
    4:    44198b3c0a4e6e44e287f4cb5dd085694384296bfcacddaecaf56687bf159da3
    5:    b43bc5459931176c371c1569b0811aee93cdd8aa39b244202b29f1f64aa9c263
Peer Timestamps:
    1585226894417, 1585207177566, 1585207177663, 1585207177511, 1585210507977,...
    1585207177561, 1585207177663, 1585207177746, 1585207177520}
```

```
Block Height:    774423
Block Hash:    0000000002296bbf32f54cea44b3c18e0df2518c90656a8d1a1f13b33ef87bb4
Prev Hash:    00000000018c5574ac89b84e3f4a03ae7ea05234d12f47d5f7a03bba59e7ceaa
Miner Time:    1585207164
FORK - last hash: 0000000003071428ba122b81ba5ebb9a349acb5871f28d6f32195d429d261eb9
Transactions:
    0:    0e13a2933fc923c119dad63abe10a5e692890a026b3554e780e5a18feb895de9
    1:    bdb29aa7a235322afacc790845e95688f8eec43ffd709fe558578ba5344a9a2b
    2:    b43bc5459931176c371c1569b0811aee93cdd8aa39b244202b29f1f64aa9c263
Peer Timestamps:
    1585207178097
    1585207178354
```


Block Height: 774423
Block Hash: 0000000003071428ba122b81ba5ebb9a349acb5871f28d6f32195d429d261eb9
Prev Hash: 00000000018c5574ac89b84e3f4a03ae7ea05234d12f47d5f7a03bba59e7ceaa
Miner Time: 1585207159
Transactions:
Coinbase: d50f910d78e21cb0daa9082b6dde491bb197a0b8bef094572568b3750b3146fd
1: bdb29aa7a235322afacc790845e95688f8eec43ffd709fe558578ba5344a9a2b
2: 32f6f261ce6a9acc0aeb396bb3112770c9a44b79cdb12c6ff270edd8da158cc6
3: a525767caaedd9eb2422117eb192fc1786e19f41ee2f01227ad1a75003a97dd9
4: 44198b3c0a4e6e44e287f4cb5dd085694384296bfcacddaecaf56687bf159da3
5: b43bc5459931176c371c1569b0811aee93cdd8aa39b244202b29f1f64aa9c263
Peer Timestamps:
{ 1585226894417, 1585207177566, 1585207177663, 1585207177511, 1585210507977,
1585207177561, 1585207177663, 1585207177746, 1585207177520 }
Block Height: 774423 [fork detected]
Block Hash: 0000000002296bbf32f54cea44b3c18e0df2518c90656a8d1a1f13b33ef87bb4
Prev Hash: 00000000018c5574ac89b84e3f4a03ae7ea05234d12f47d5f7a03bba59e7ceaa
Miner Time: 1585207164
Transactions:
Coinbase: 0e13a2933fc923c119dad63abe10a5e692890a026b3554e780e5a18feb895de9
1: bdb29aa7a235322afacc790845e95688f8eec43ffd709fe558578ba5344a9a2b
2: b43bc5459931176c371c1569b0811aee93cdd8aa39b244202b29f1f64aa9c263
Peer Timestamps:
{ 1585207178097, 1585207178354 }


1e7
4.0
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0.0
raw_prop_ms
782600
782800
783000
783200
783400
block_height
Zcash Foundation
INSIGHT
[accidental discovery:] Can see the exact sync time per block for a remote node booting up.