Visualizing Monero:
A figure is worth a thousand logs

Isthmus (Mitchell Krawiec-Thayer) & Neptune

Outline:

- Intro
  - Motivation
  - Anonymity pools and puddles
  - Transaction tree analysis heuristics
- Act I: Unusual fees
- Act II: Juvenile ring members
- Act III: Egregious decoy selection

Motivation

- Keep Monero users safe

Motivation

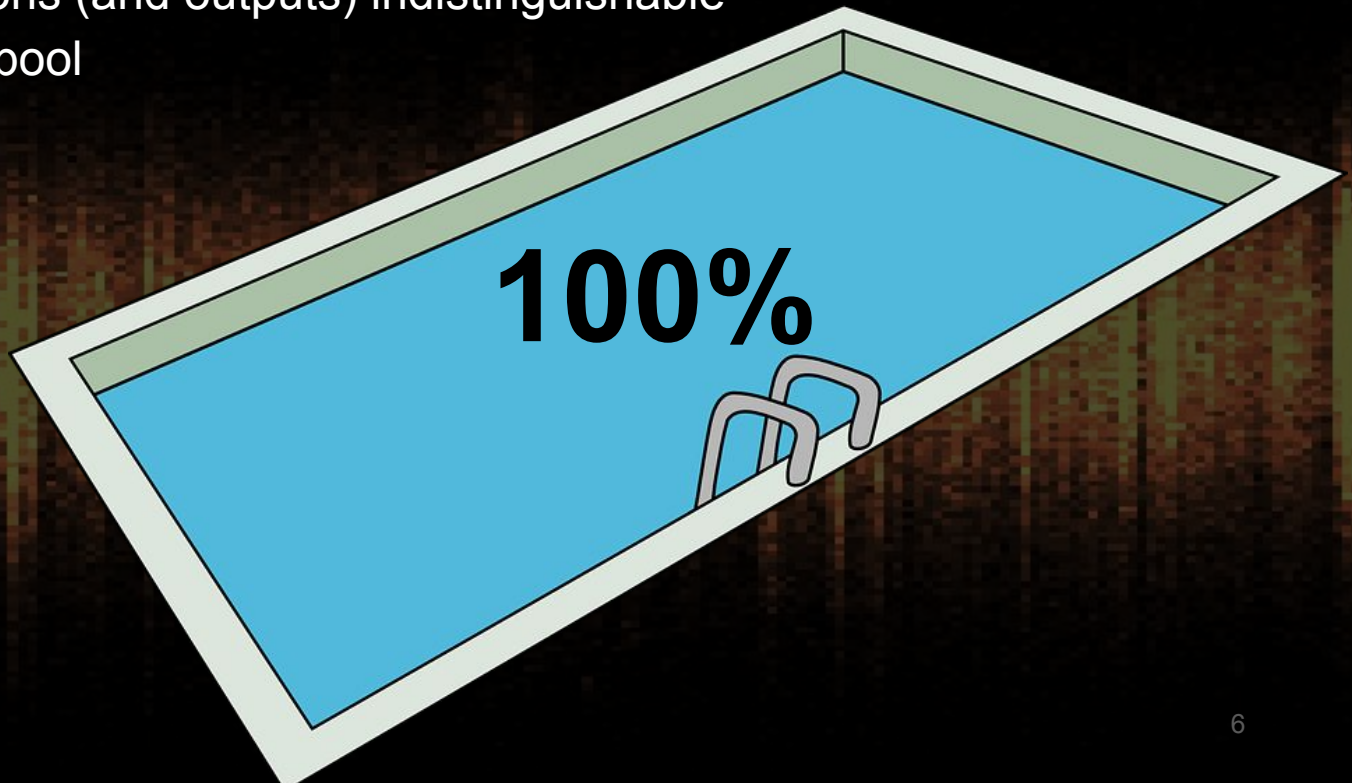
- Keep Monero users safe
- Inform best practices for users
- Inform best practices for software creators

Motivation

- Keep Monero users safe
- Inform best practices for users
- Inform best practices for software creators
- Design protocol that enforces best practices…
- … by identifying and preventing anomalous behaviors

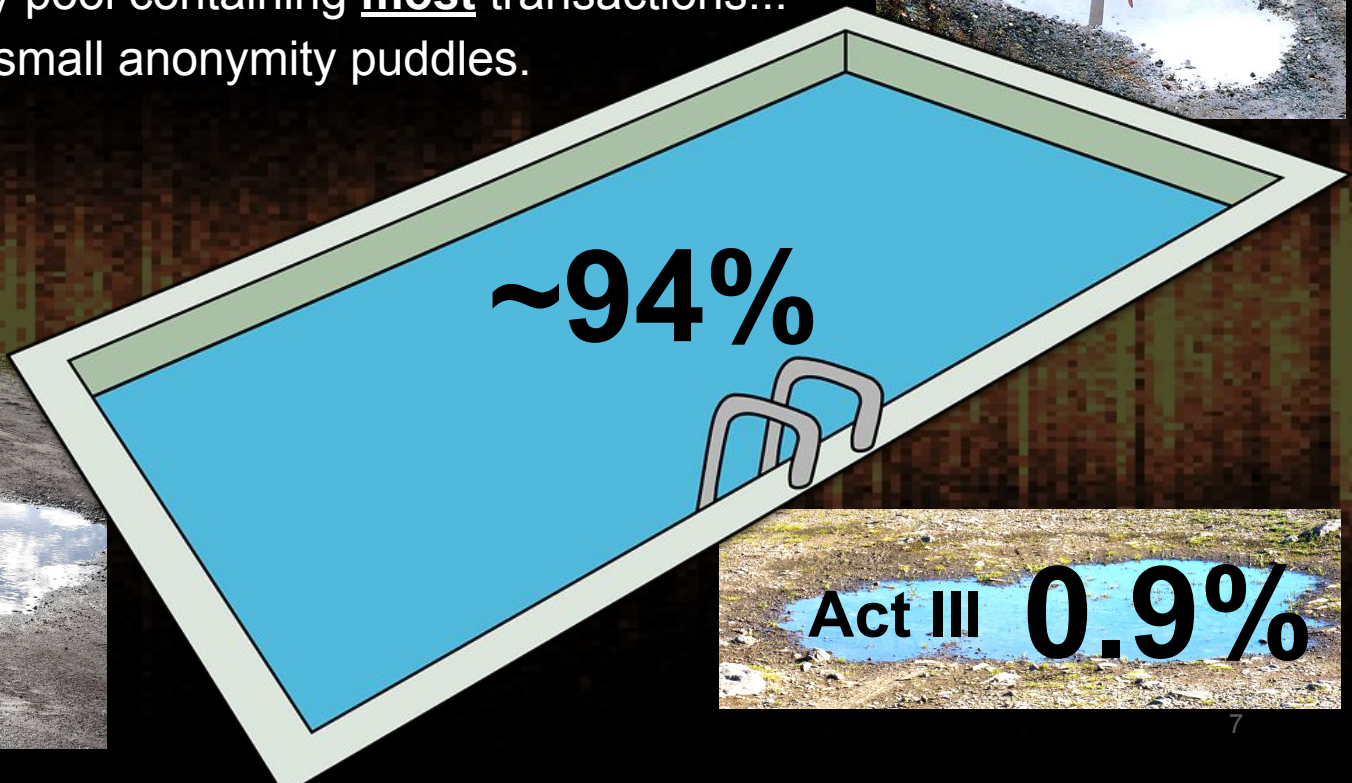
Monero ideal:

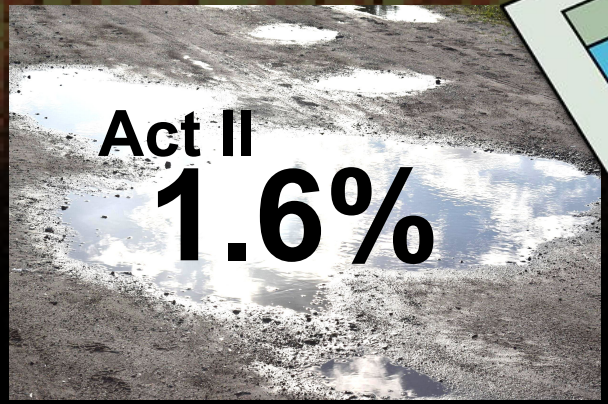
- 100% of transactions (and outputs) indistinguishable
- Single anonymity pool



Monero to a cynical statistician:

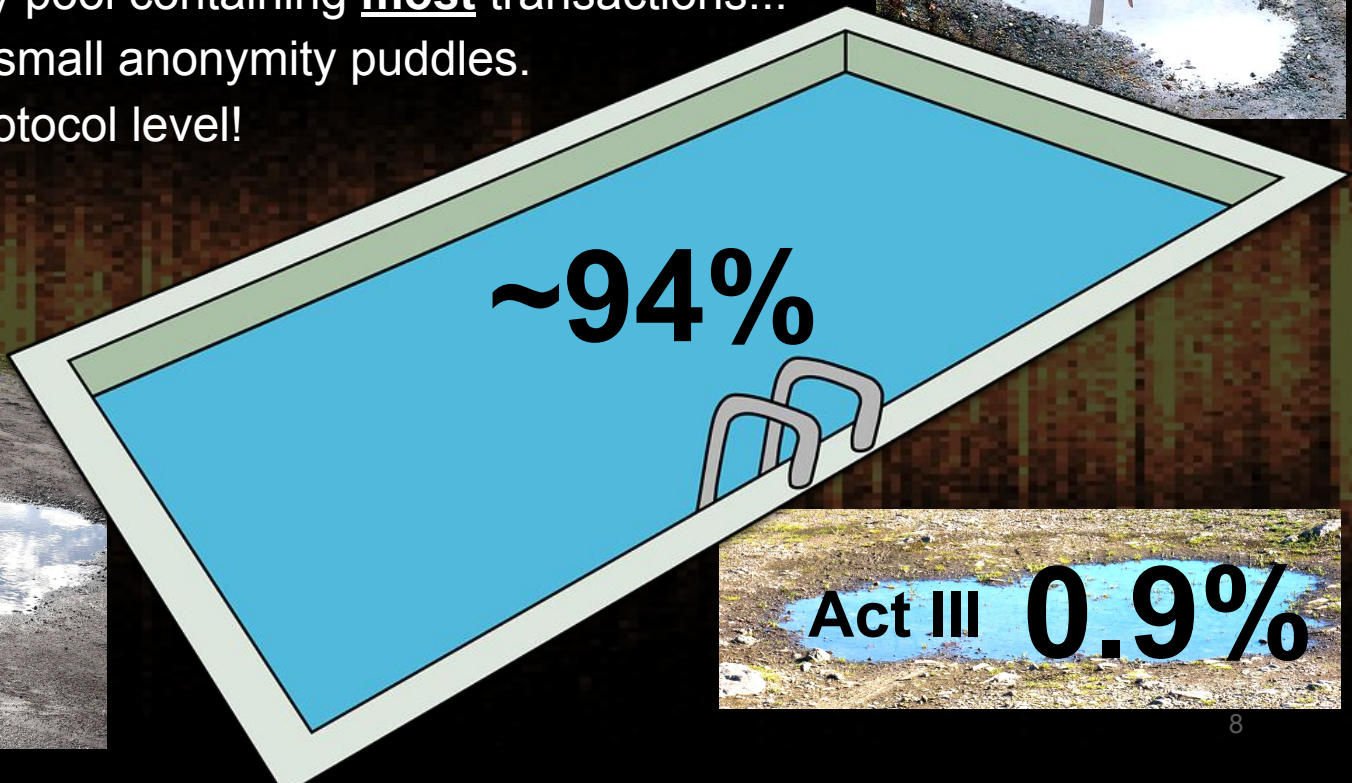
- One big anonymity pool containing **most** transactions...
- … surrounded by small anonymity puddles.

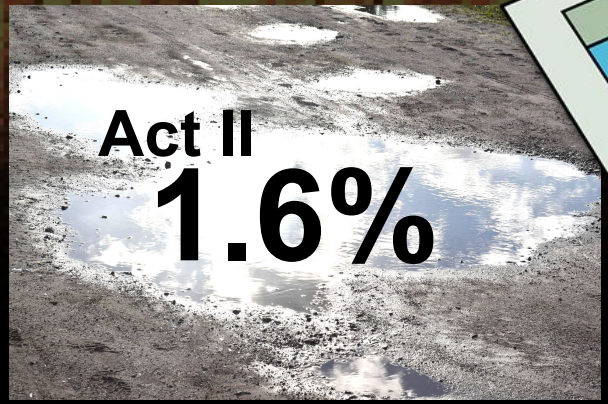




Monero to a cynical statistician:

- One big anonymity pool containing **most** transactions...
- … surrounded by small anonymity puddles.
- Can be fixed at protocol level!





Note: you are probably in the main pool
(unless you use custom software)

~94%

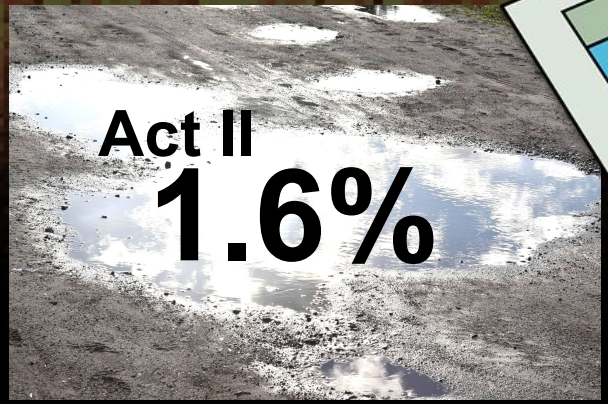


Diagram simplifications:
1-in / 1-out transactions (norm is 1+/2+)
Ring size 3 (reality is 11)

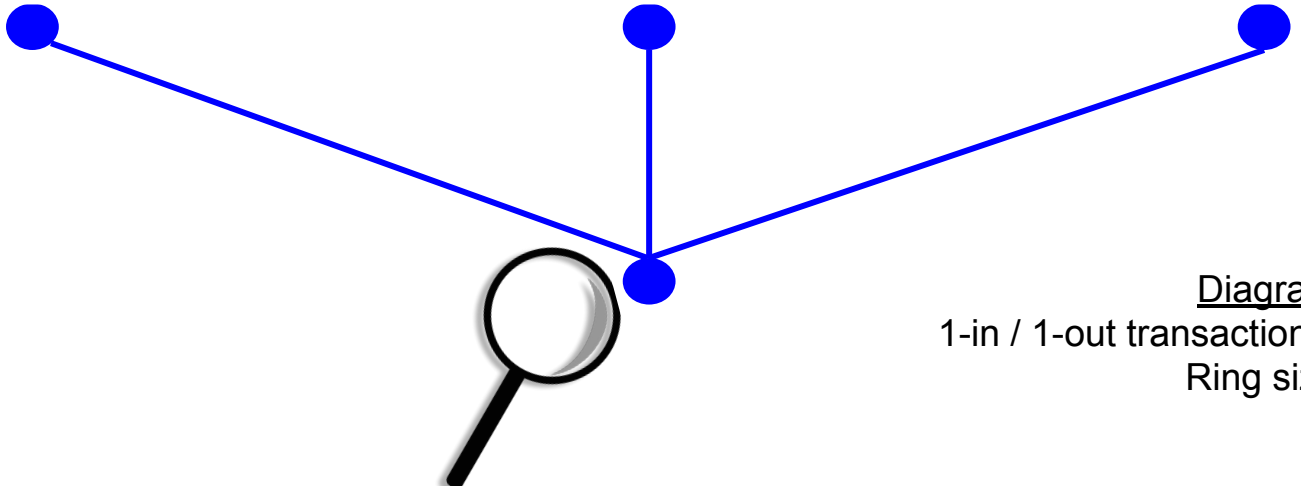


Diagram simplifications:
1-in / 1-out transactions (norm is 1+/2+)
Ring size 3 (reality is 11)

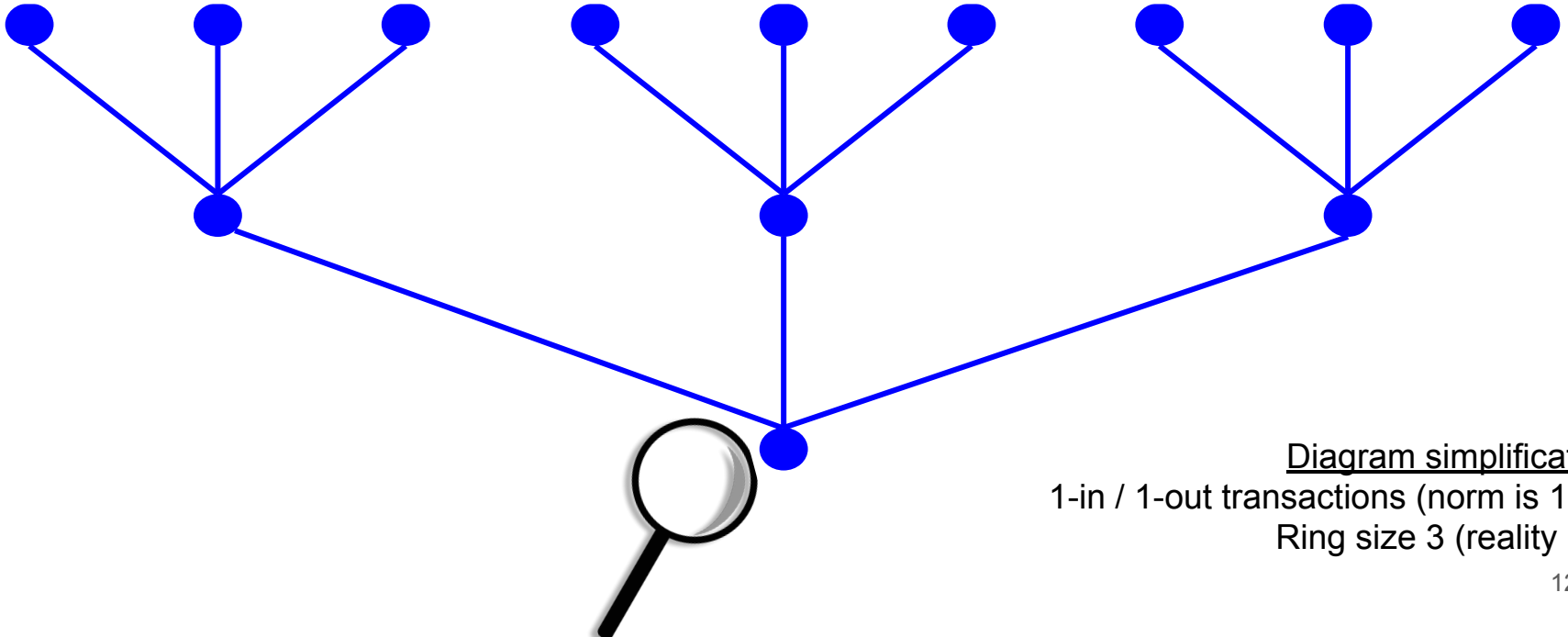


Diagram simplifications:
1-in / 1-out transactions (norm is 1+/2+)
Ring size 3 (reality is 11)

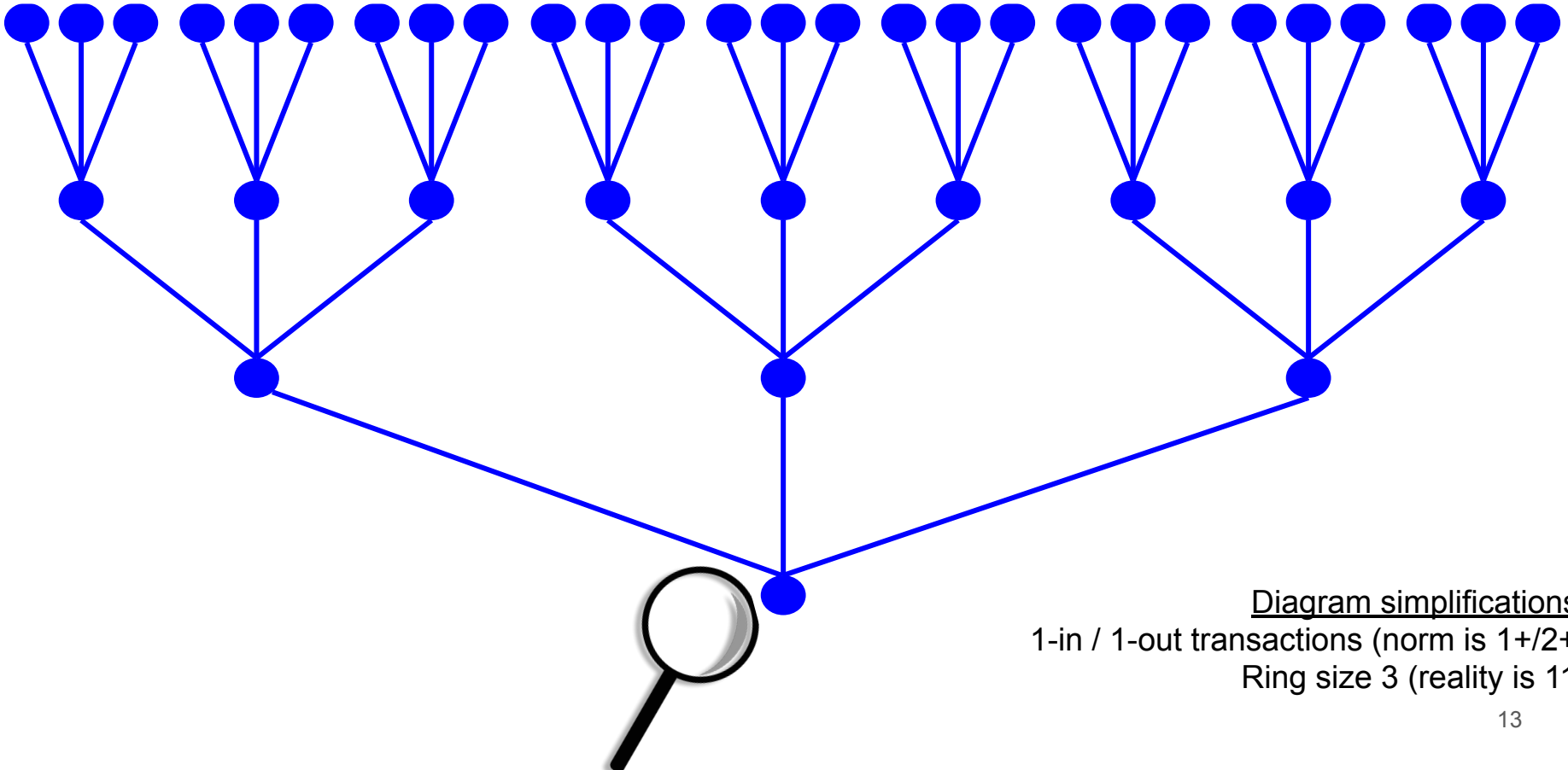


Diagram simplifications:
1-in / 1-out transactions (norm is 1+/2+)
Ring size 3 (reality is 11)

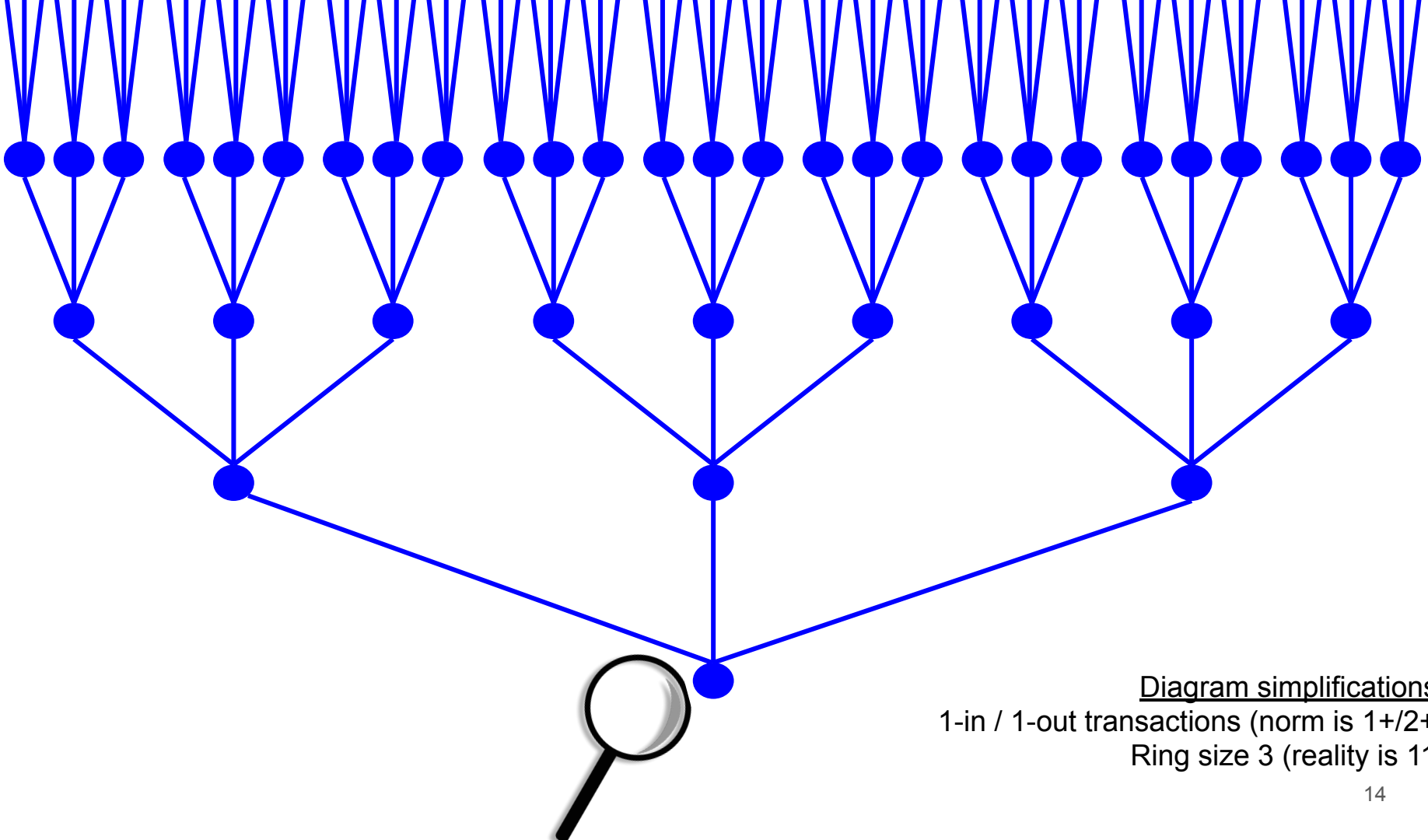


Diagram simplifications:
1-in / 1-out transactions (norm is 1+/2+)
Ring size 3 (reality is 11)

Blue circles = ideal (100% indistinguishable anonymity pool)

<u>Diagram simplifications:</u>
1-in / 1-out transactions (norm is 1+/2+)
Ring size 3 (reality is 11)

Blue circles = ideal (100% indistinguishable anonymity pool)
Red squares = transactions with distinguishing feature(s)

Many possible types of fungibility defects for privacy coins:

Blue circles = ideal (100% indistinguishable anonymity pool)
Red squares = transactions with distinguishing feature(s)

Many possible types of fungibility defects for privacy coins:

- Anomalous ring size (fixed in v8)

Blue circles = ideal (100% indistinguishable anonymity pool)
Red squares = transactions with distinguishing feature(s)

Many possible types of fungibility defects for privacy coins:

- Anomalous ring size (fixed in v8)
- Tx_extra contents and metadata (PID & Neptune analysis)

Blue circles = ideal (100% indistinguishable anonymity pool)
Red squares = transactions with distinguishing feature(s)

Many possible types of fungibility defects for privacy coins:

- Anomalous ring size (fixed in v8)
- Tx_extra contents and metadata (PID & Neptune analysis)
- Anomalous transaction structure (e.g. single-output txns)

Blue circles = ideal (100% indistinguishable anonymity pool)
Red squares = transactions with distinguishing feature(s)

Many possible types of fungibility defects for privacy coins:

- Anomalous ring size (fixed in v8)
- Tx_extra contents and metadata (PID & Neptune analysis)
- Anomalous transaction structure (e.g. single-output txns)
- Anomalous fees (*this talk, Act I*)

Blue circles = ideal (100% indistinguishable anonymity pool)
Red squares = transactions with distinguishing feature(s)

Many possible types of fungibility defects for privacy coins:

- Anomalous ring size (fixed in v8)
- Tx_extra contents and metadata (PID & Neptune analysis)
- Anomalous transaction structure (e.g. single-output txns)
- Anomalous fees (*this talk, Act I*)
- Ignore unenforced lock time (*this talk, Act II*)

Blue circles = ideal (100% indistinguishable anonymity pool)
Red squares = transactions with distinguishing feature(s)

Many possible types of fungibility defects for privacy coins:

- Anomalous ring size (fixed in v8)
- Tx_extra contents and metadata (PID & Neptune analysis)
- Anomalous transaction structure (e.g. single-output txns)
- Anomalous fees (*this talk, Act I*)
- Ignore unenforced lock time (*this talk, Act II*)
- Incorrect ring member selection (*this talk, Act III*)

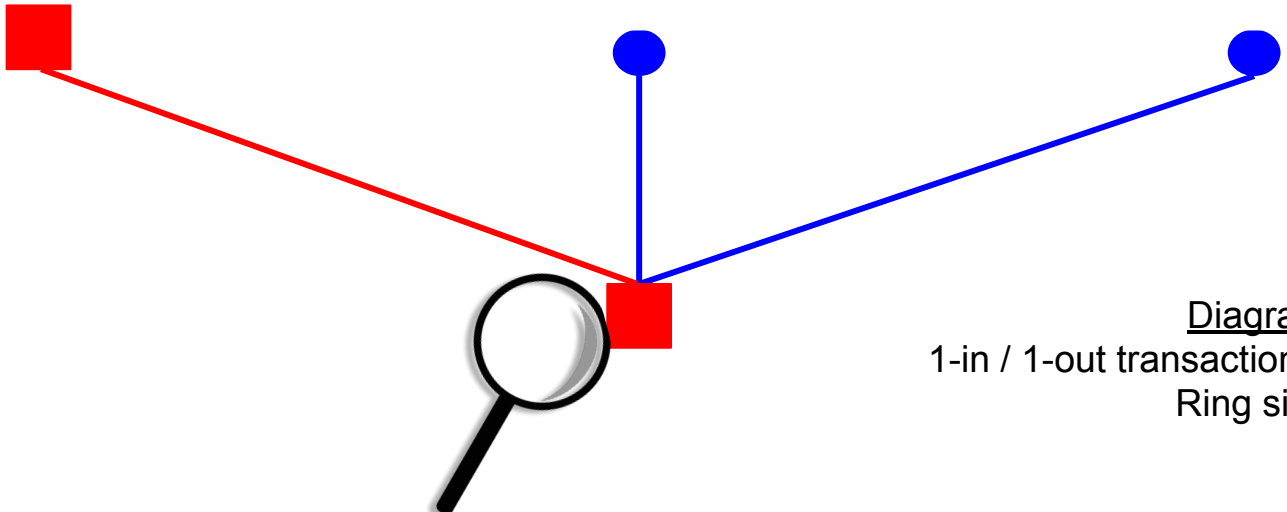


Diagram simplifications:
1-in / 1-out transactions (norm is 1+/2+)
Ring size 3 (reality is 11)

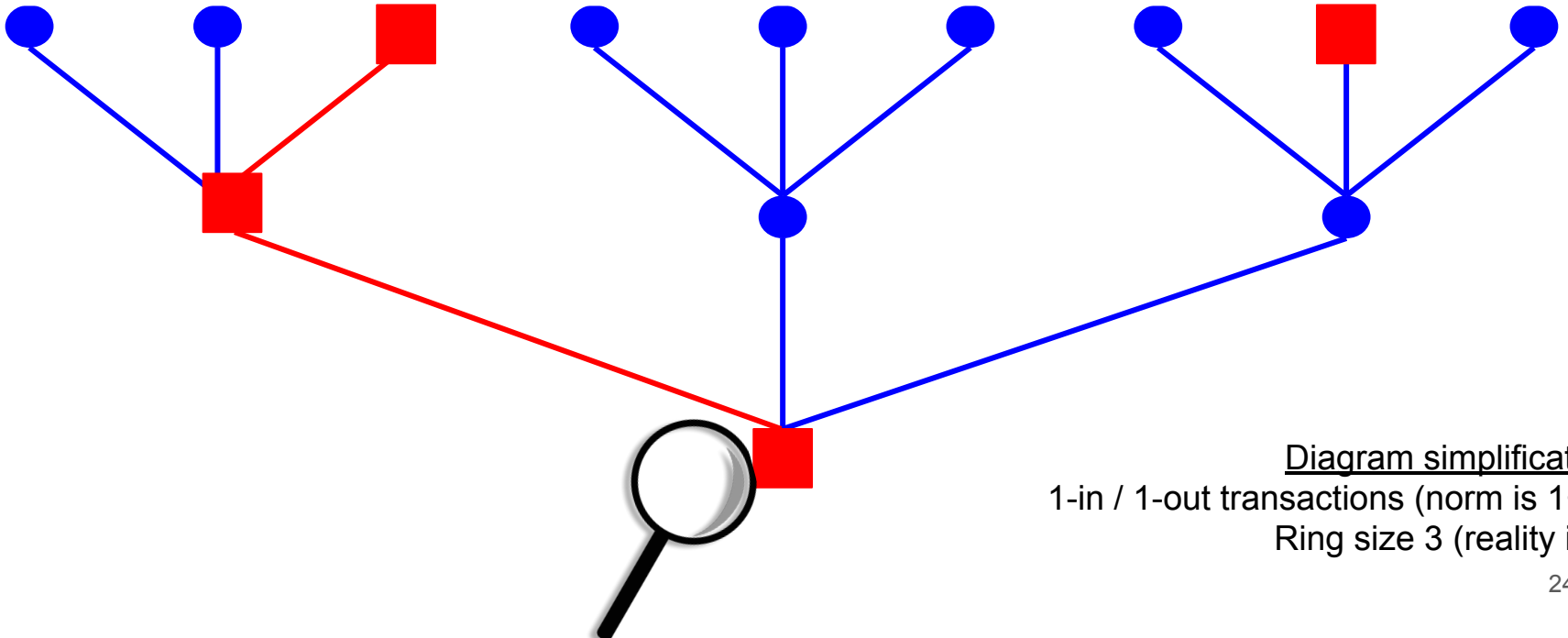


Diagram simplifications:
1-in / 1-out transactions (norm is 1+/2+)
Ring size 3 (reality is 11)

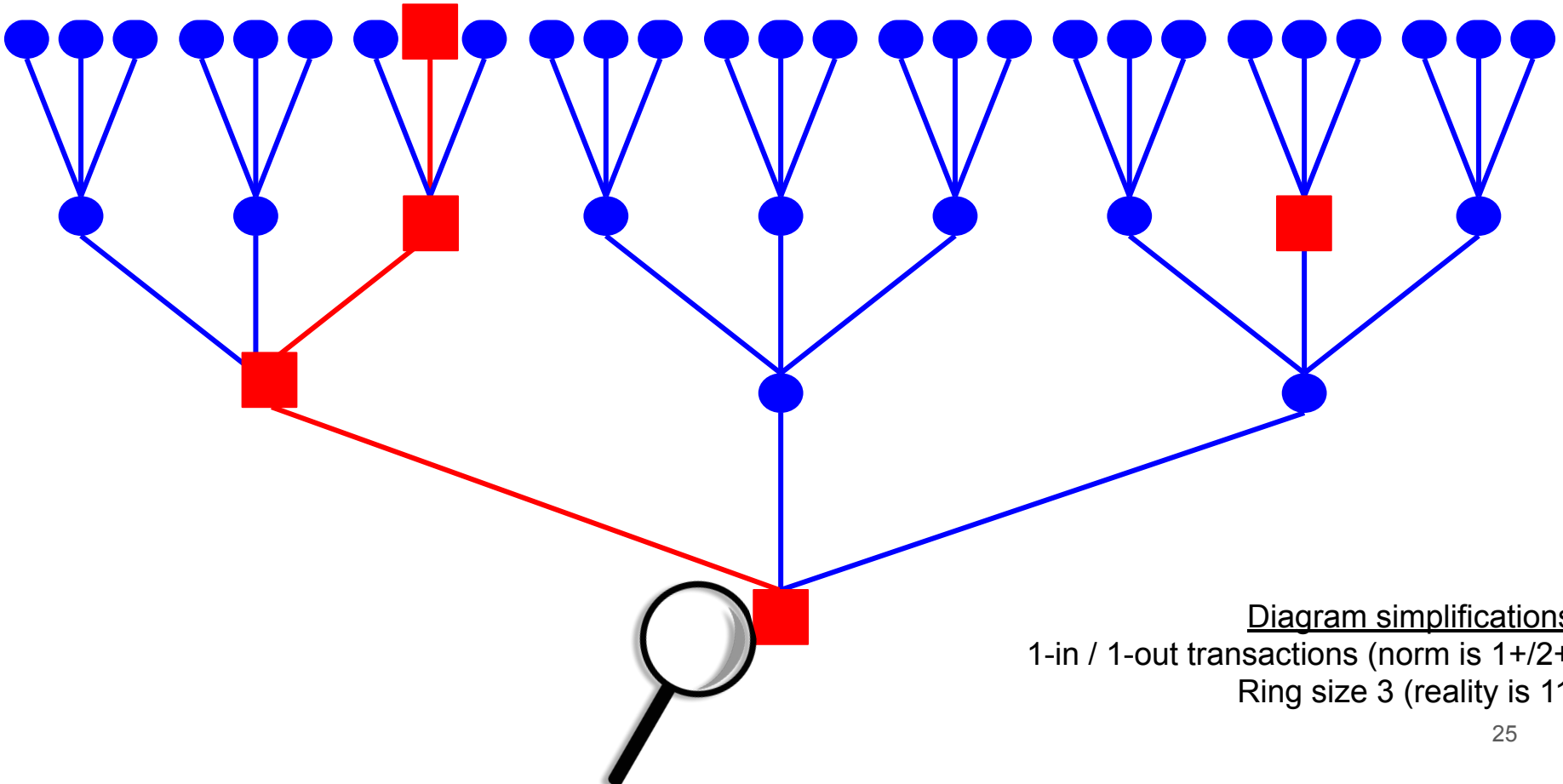


Diagram simplifications:
1-in / 1-out transactions (norm is 1+/2+)
Ring size 3 (reality is 11)

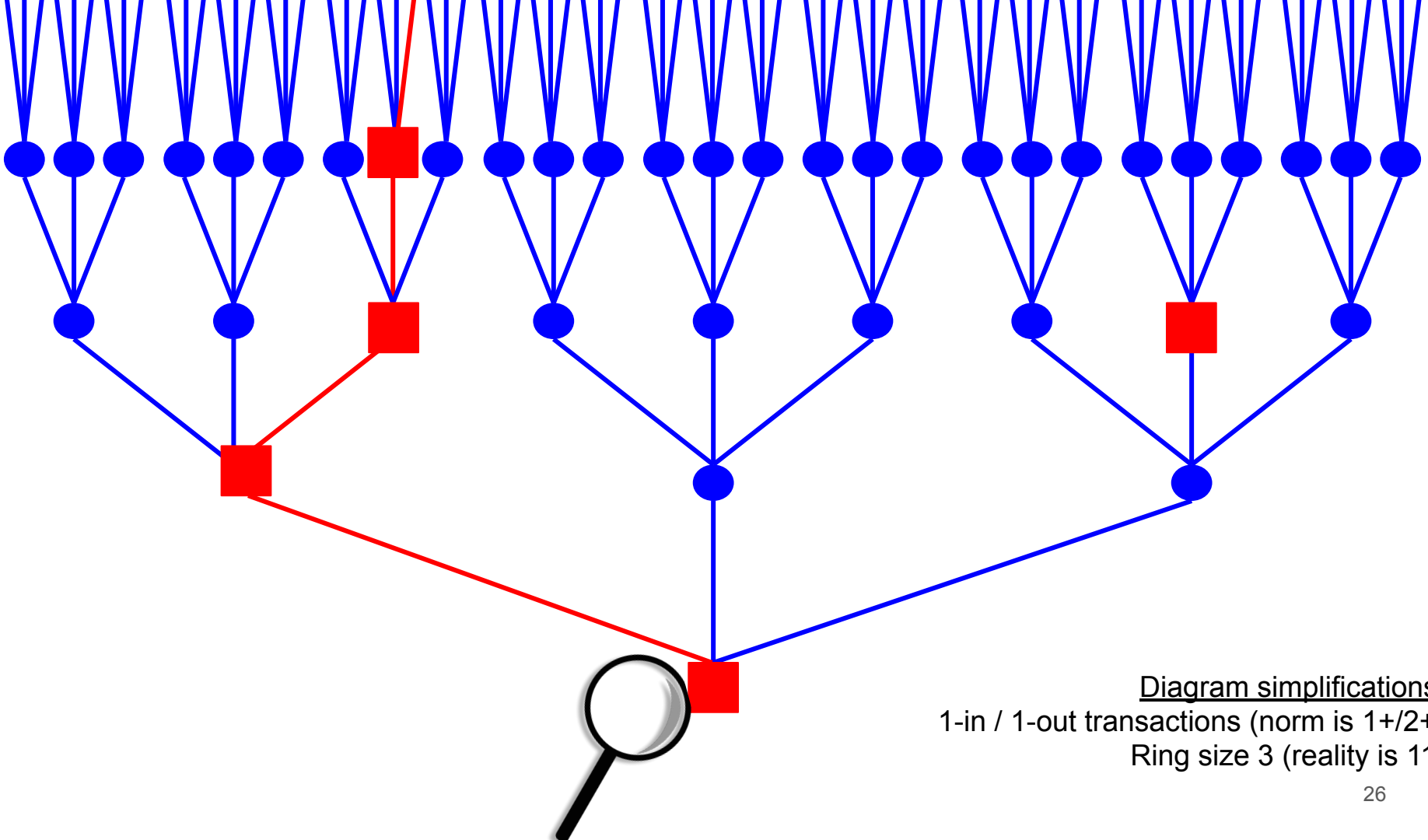
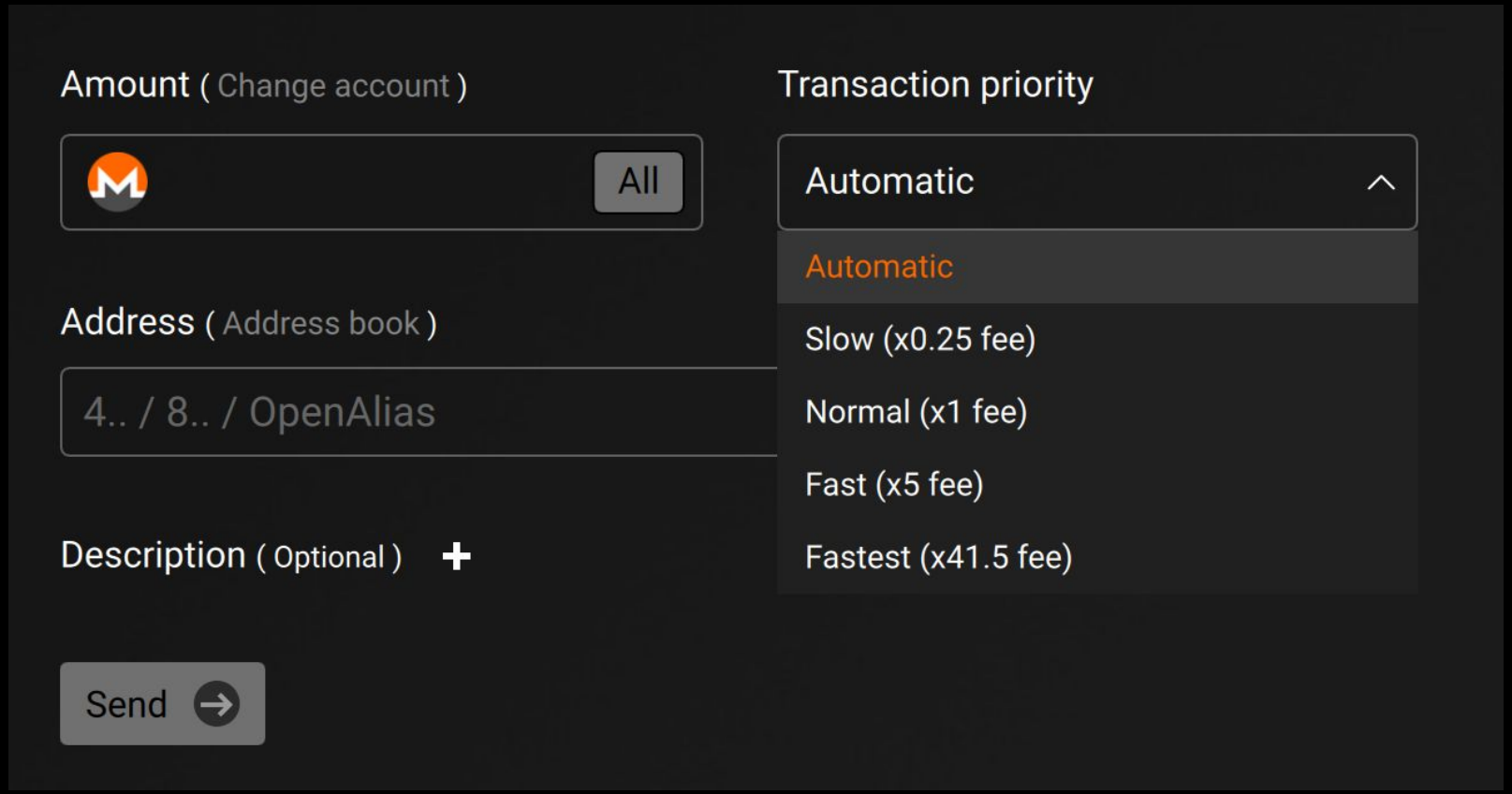
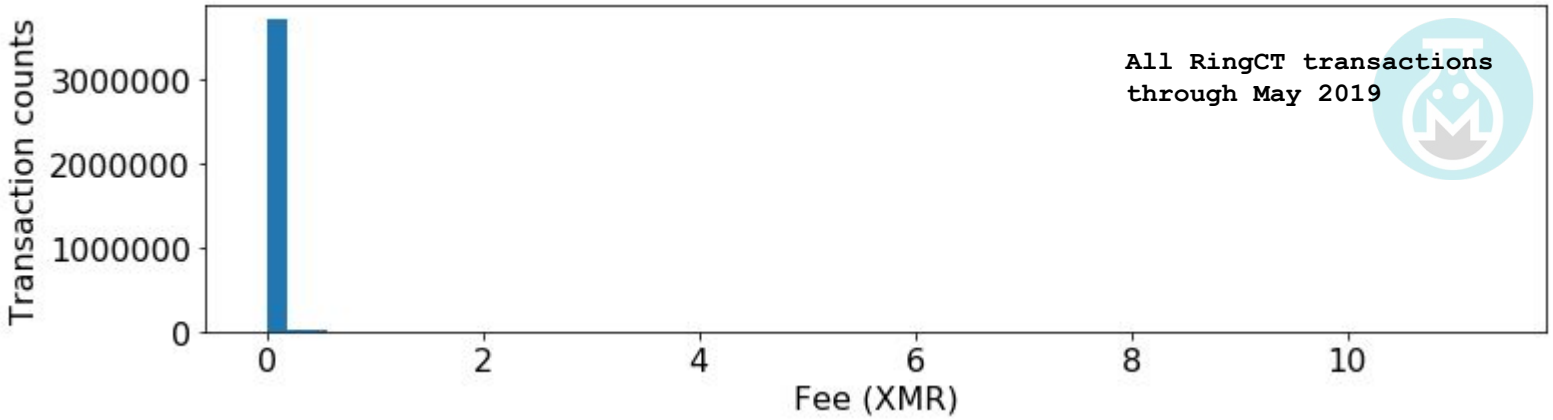


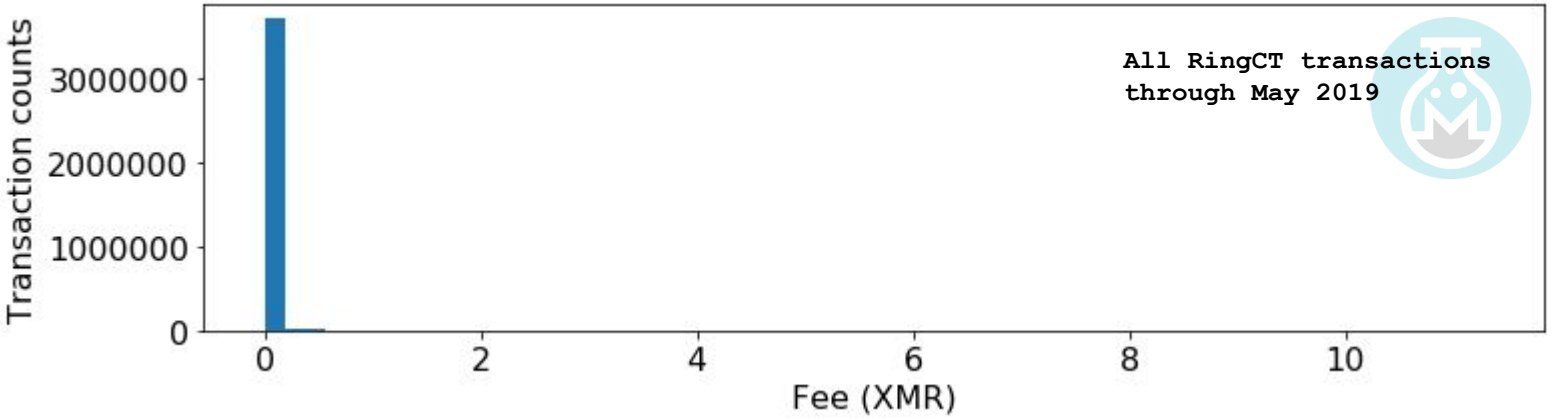
Diagram simplifications:
1-in / 1-out transactions (norm is 1+/2+)
Ring size 3 (reality is 11)

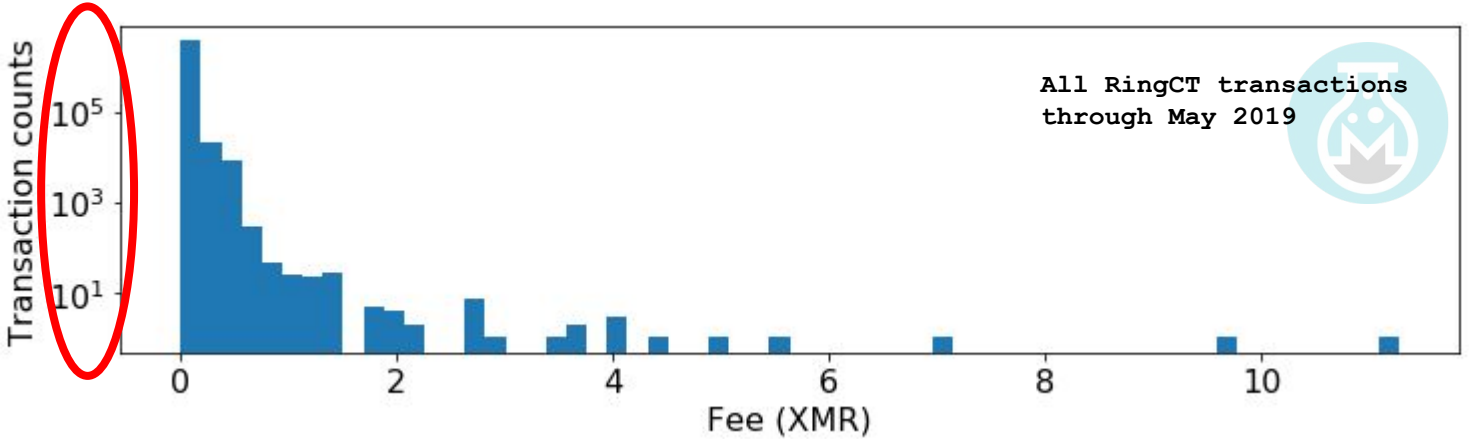
Act I

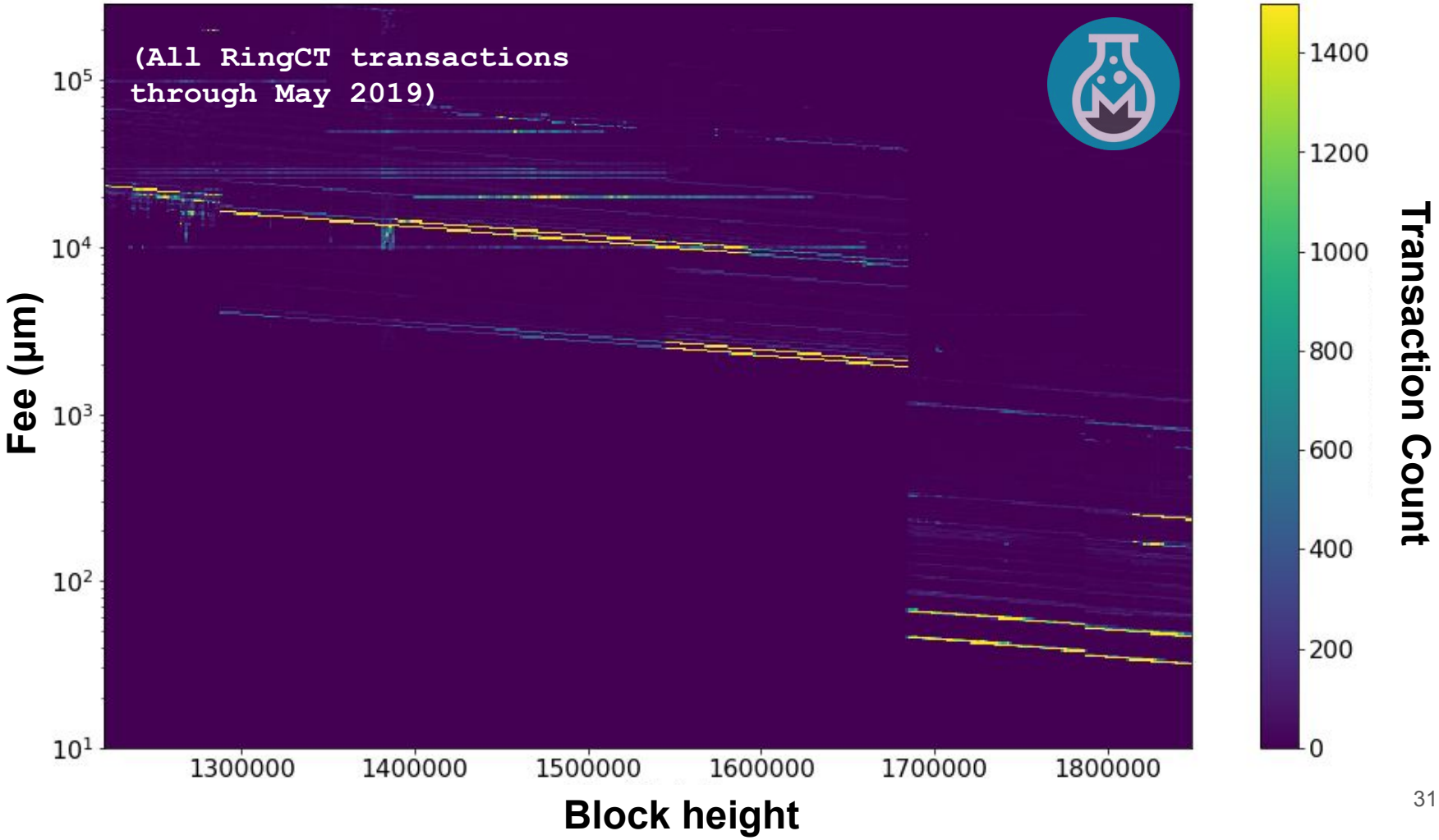
Unusual fees

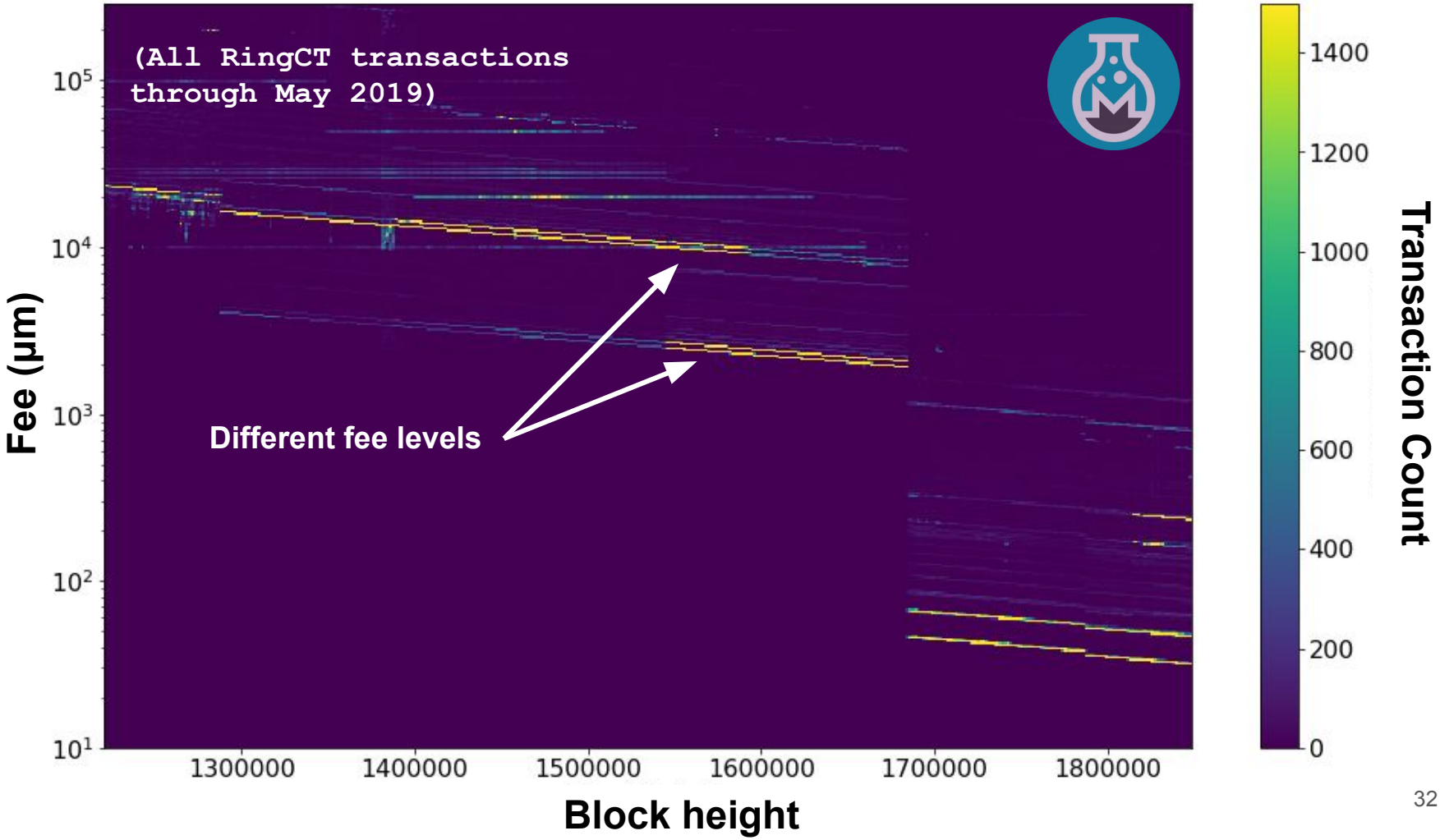

Amount (Change account)
All
Address (Address book)
4.. / 8.. / OpenAlias
Description (Optional)
Send
Transaction priority
Automatic
Automatic
Slow (x0.25 fee)
Normal (x1 fee)
Fast (x5 fee)
Fastest (x41.5 fee)

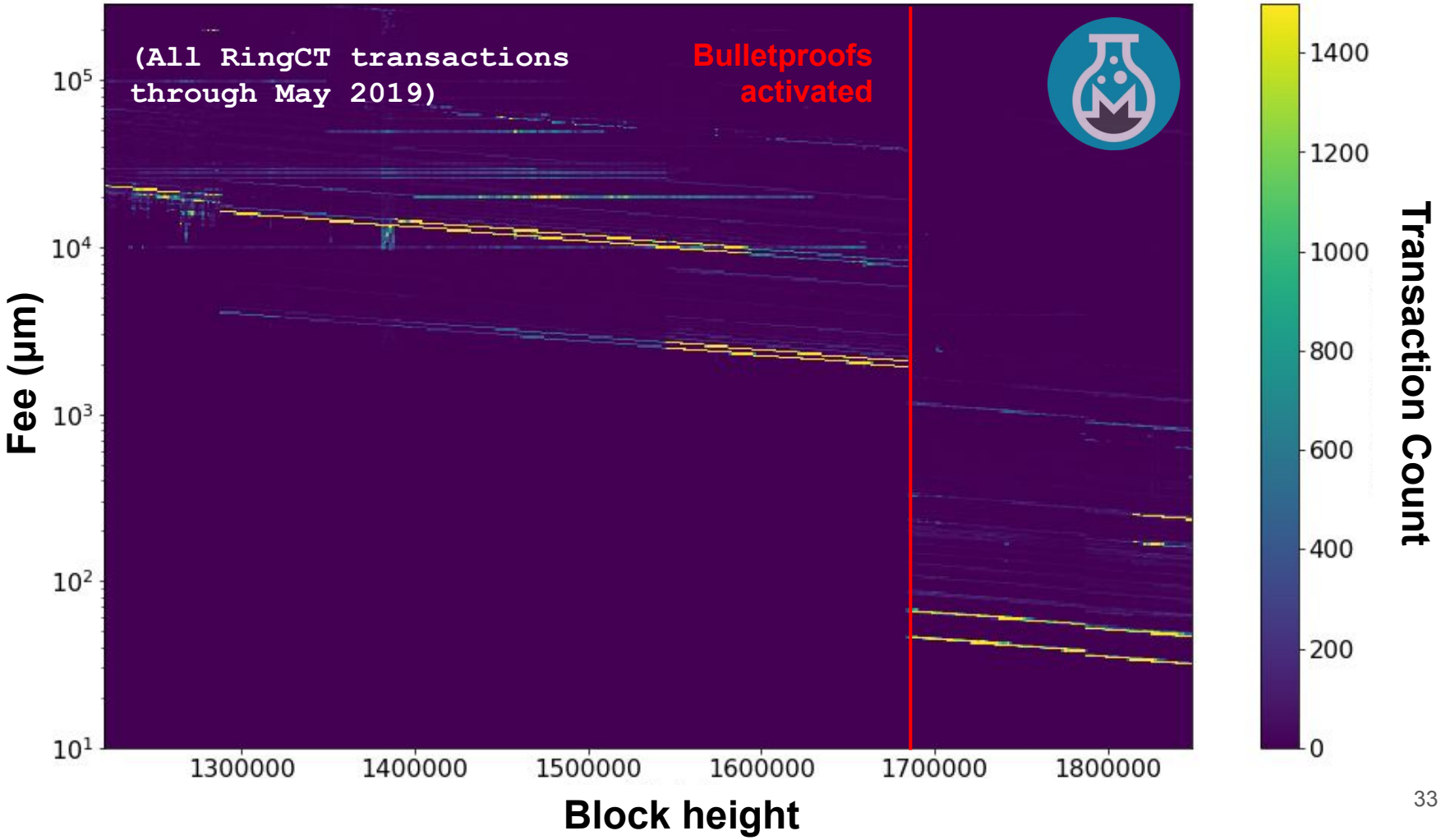

Transaction counts
3000000
2000000
1000000
0
0
2
4
6
8
10
Fee (XMR)
All RingCT transactions
through May 2019

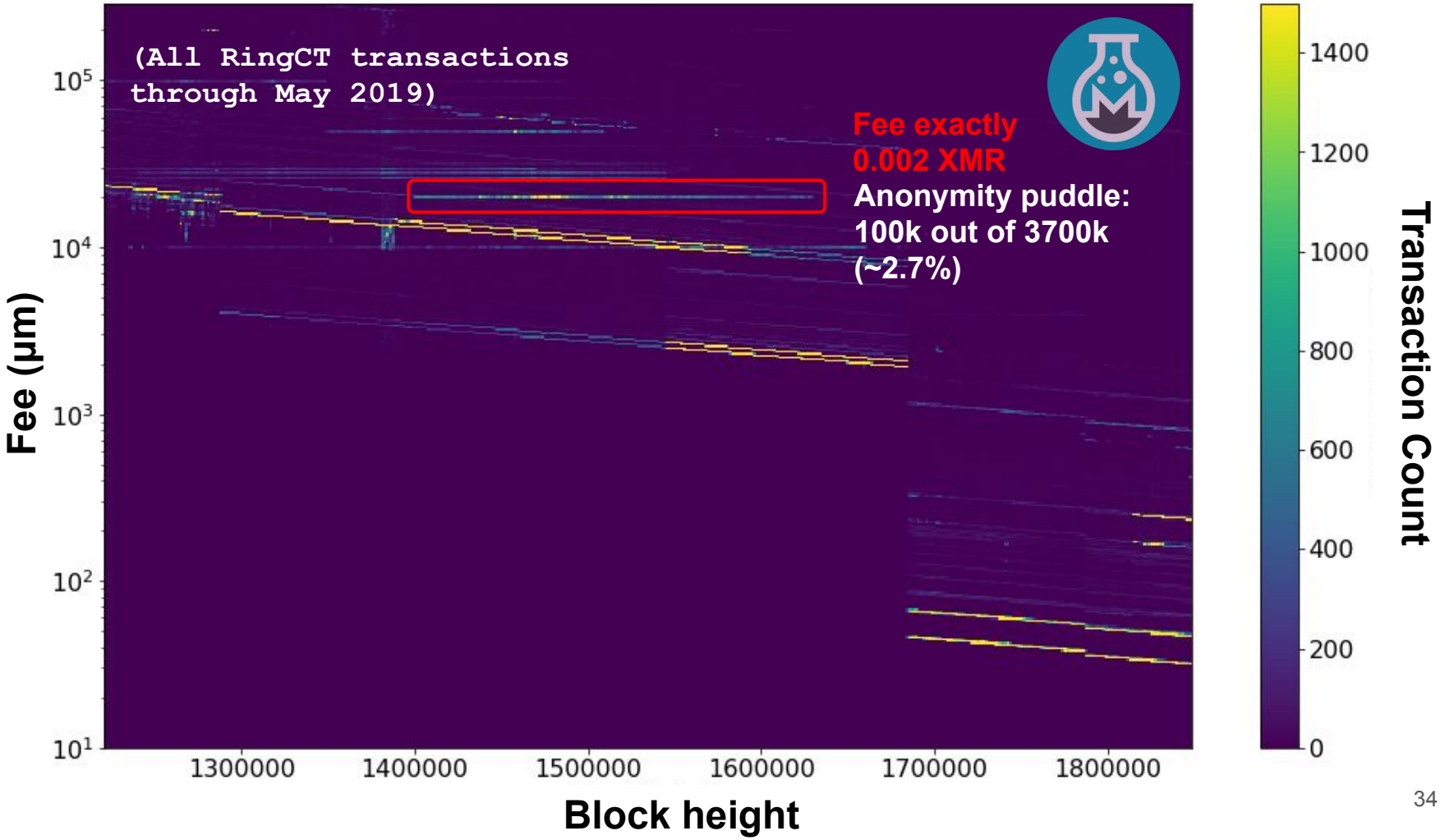

Transaction counts
3000000
2000000
1000000
0
0
2
4
6
8
10
Fee (XMR)
All RingCT transactions
through May 2019

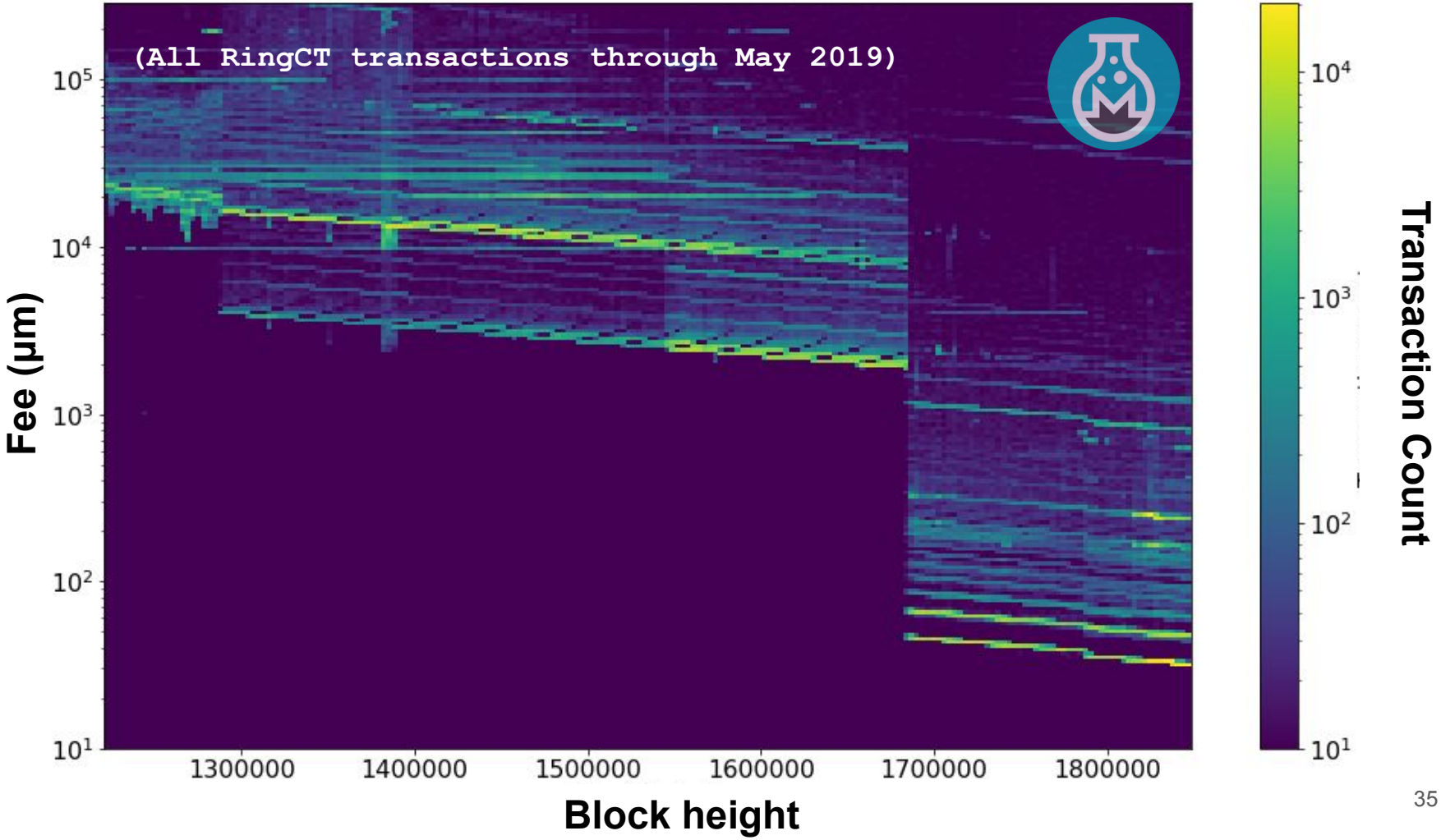

Transaction counts
10^5
10^3
10^1
0
2
4
6
8
10
Fee (XMR)
All RingCT transactions
through May 2019

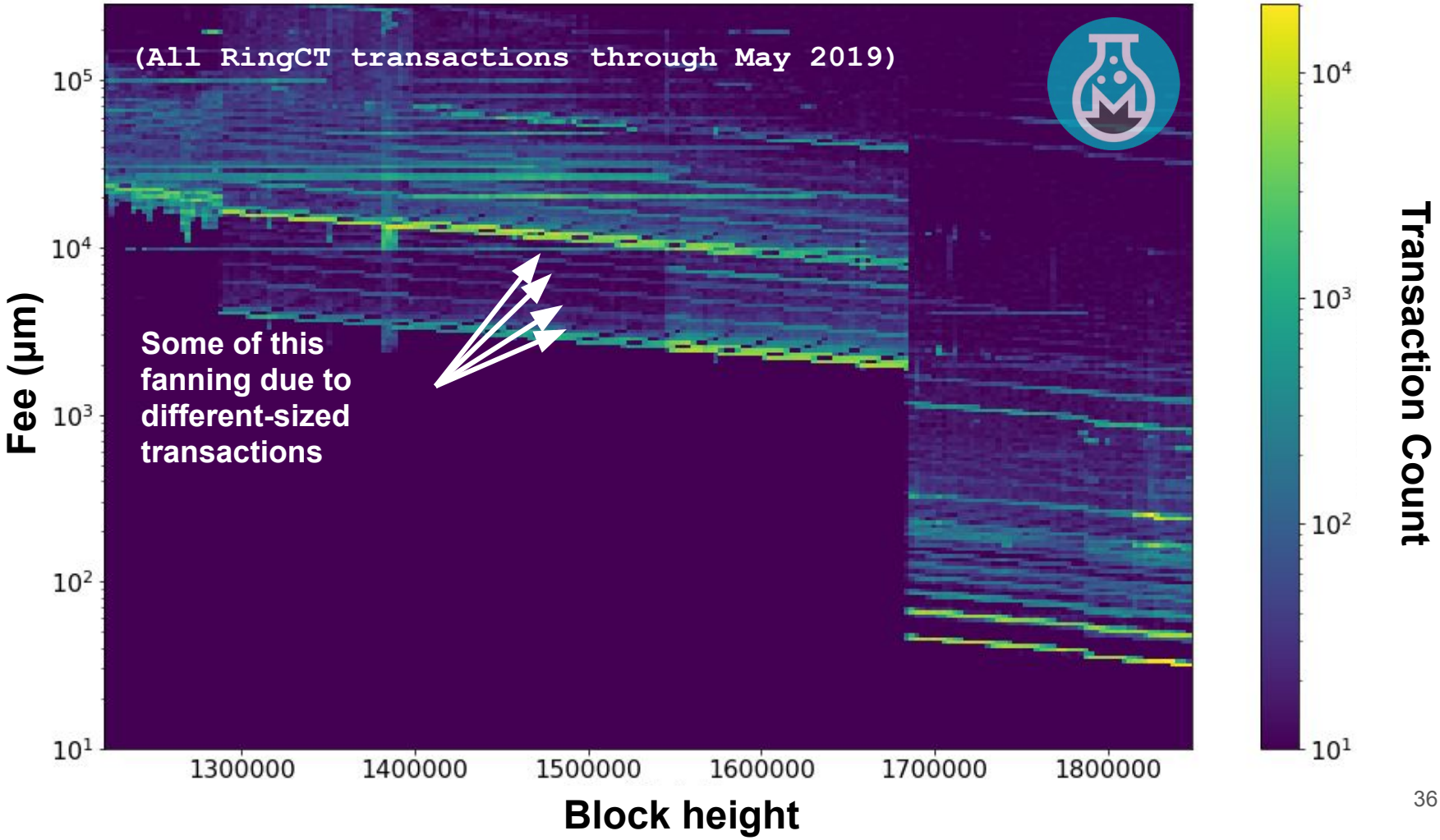

(All RingCT transactions through May 2019)
Fee (µm)
10^5
10^4
10^3
10^2
10^1
1300000
1400000
1500000
1600000
1700000
1800000
Block height
1400
1200
1000
800
600
400
200
0
Transaction Count

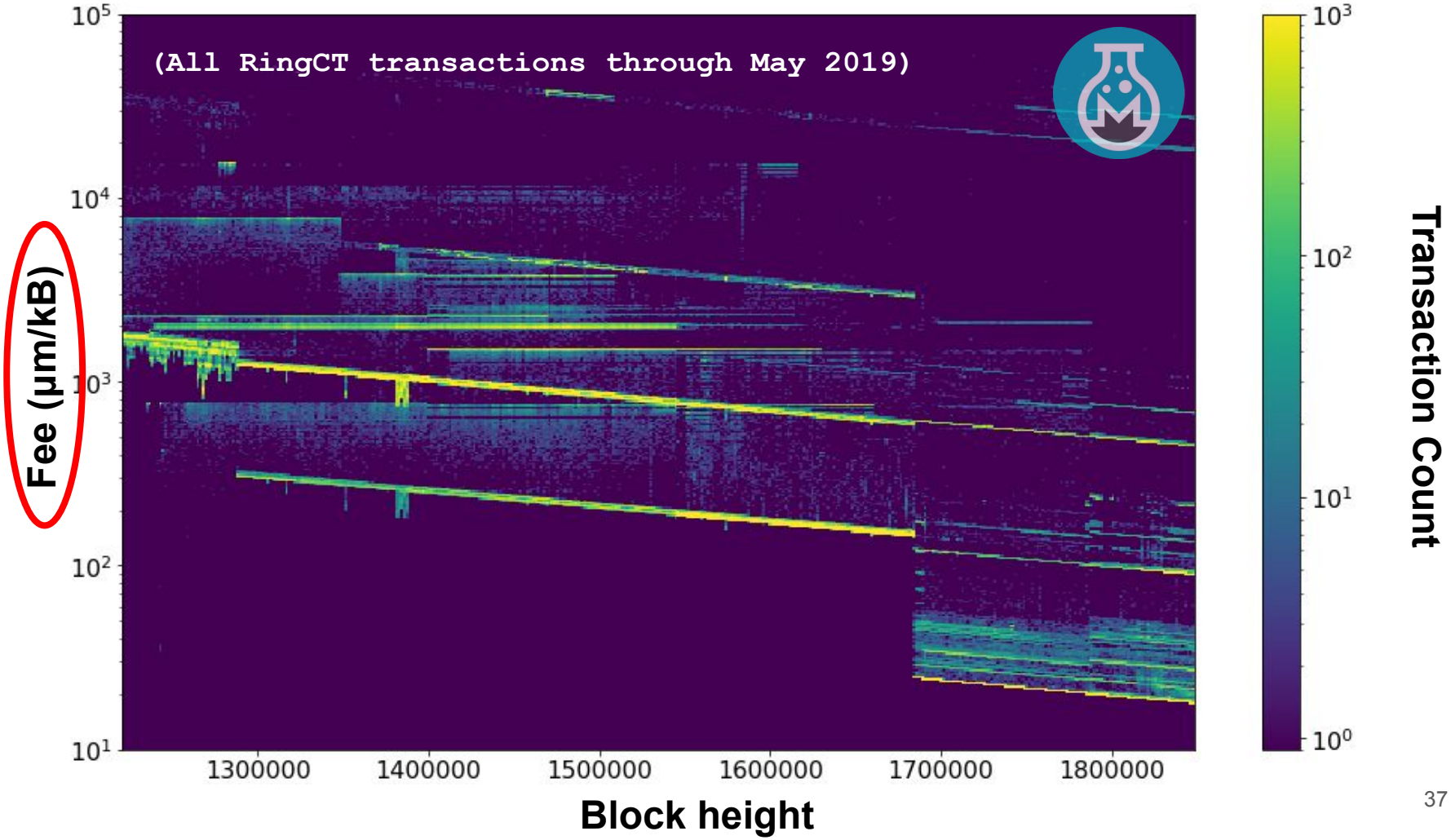

(All RingCT transactions through May 2019)
Different fee levels
Fee (µm)
10^5
10^4
10^3
10^2
10^1
1300000
1400000
1500000
1600000
1700000
1800000
Block height
1400
1200
1000
800
600
400
200
0
Transaction Count

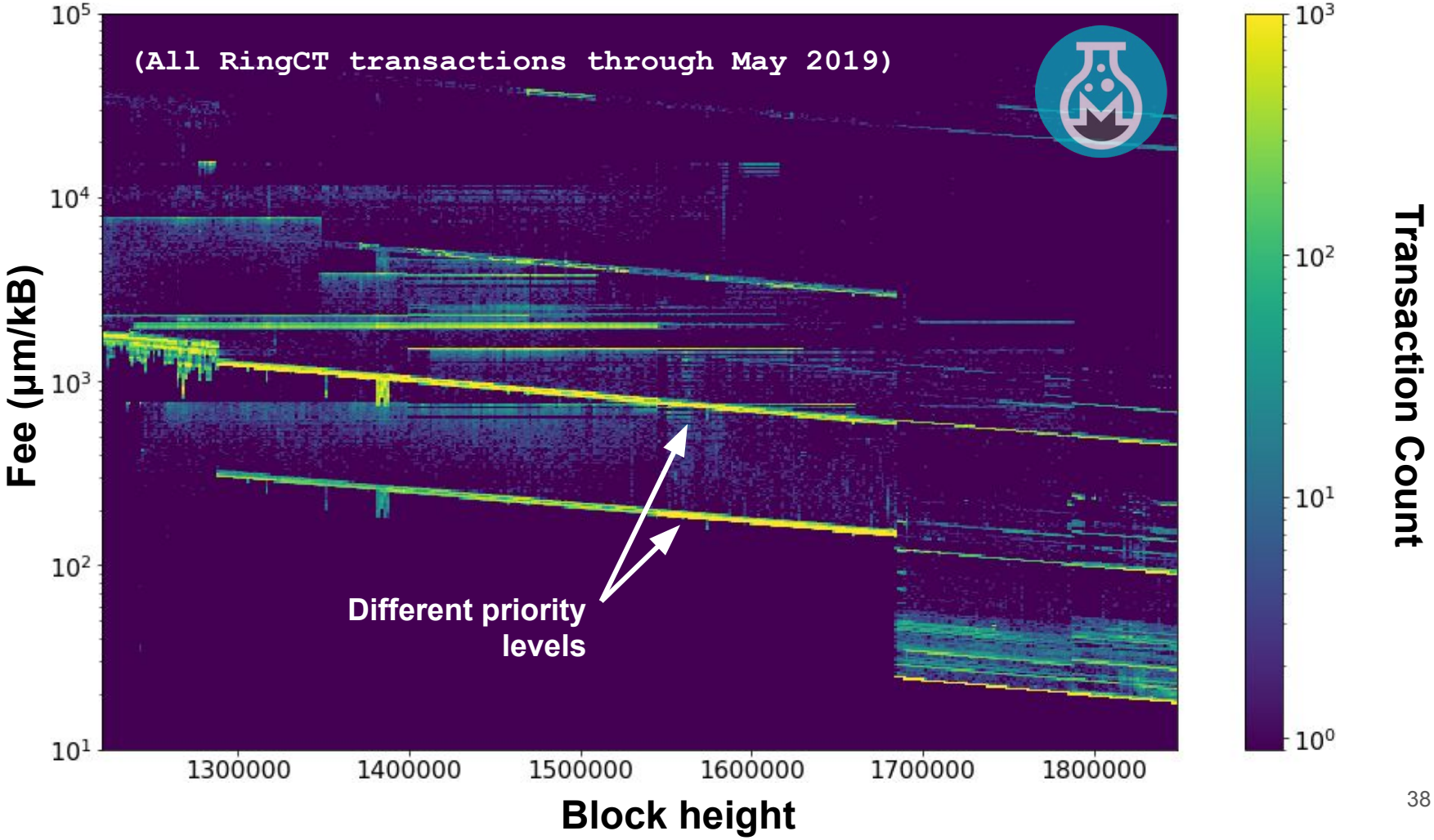

(All RingCT transactions through May 2019)
Bulletproofs activated
Fee (µm)
10^5
10^4
10^3
10^2
10^1
1300000
1400000
1500000
1600000
1700000
1800000
Block height
1400
1200
1000
800
600
400
200
0
Transaction Count

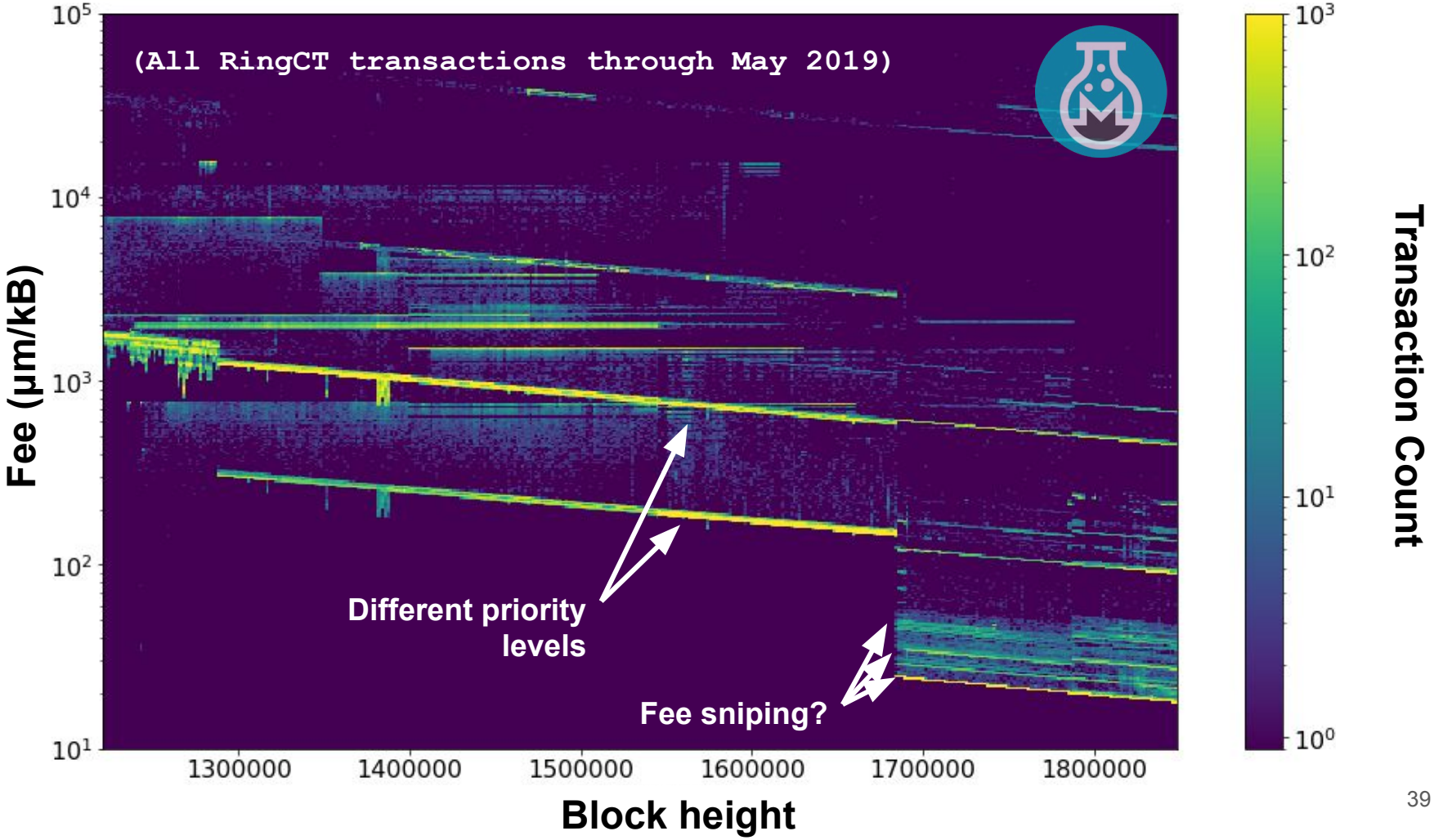

(All RingCT transactions through May 2019)
Fee exactly 0.002 XMR
Anonymity puddle: 100k out of 3700k (~2.7%)
Fee (µm)
10^5
10^4
10^3
10^2
10^1
1300000
1400000
1500000
1600000
1700000
1800000
Block height
1400
1200
1000
800
600
400
200
0
Transaction Count

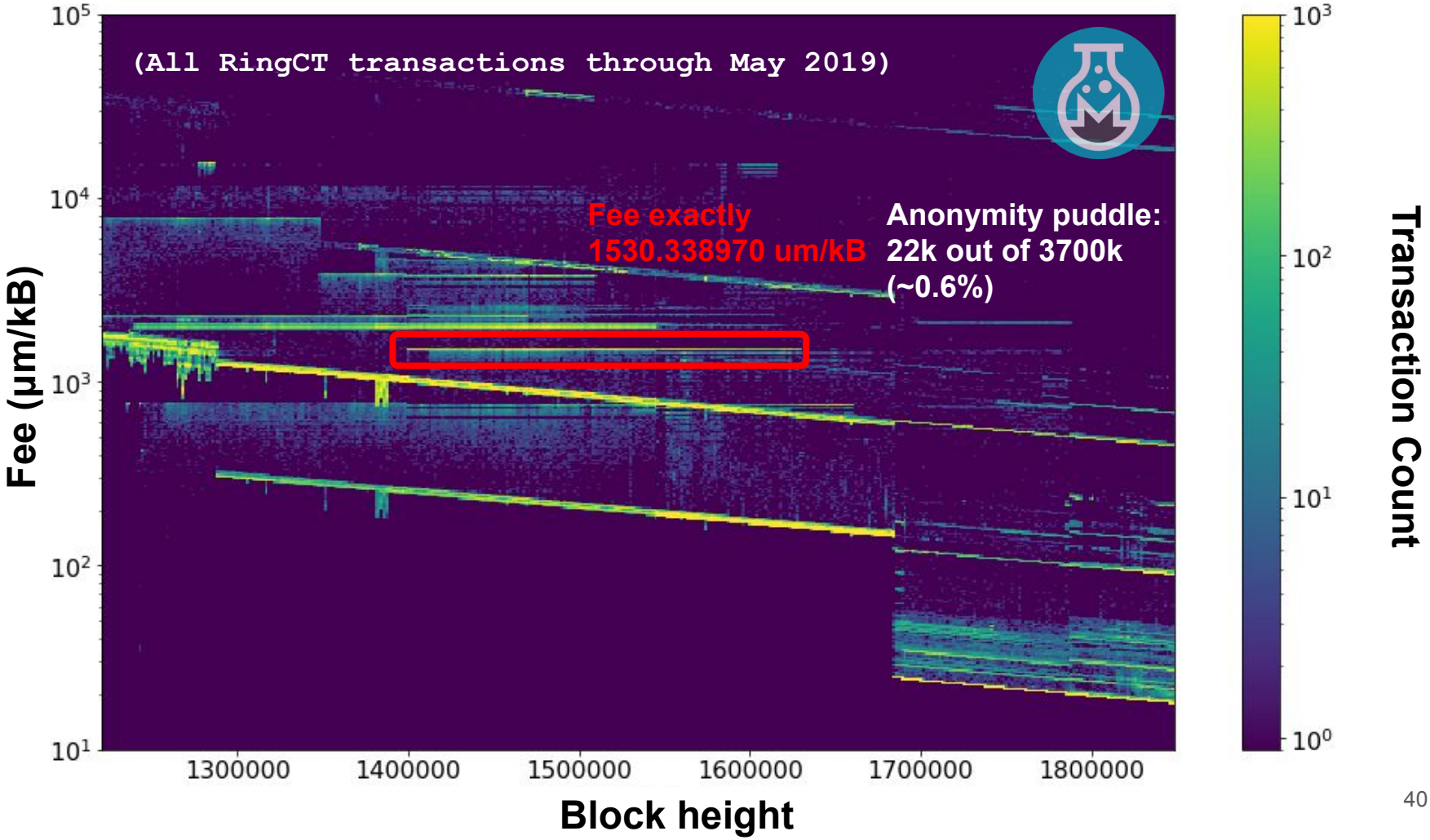

(All RingCT transactions through May 2019)
Fee (μm)
10^5
10^4
10^3
10^2
10^1
1300000
1400000
1500000
1600000
1700000
1800000
Block height
10^4
10^3
10^2
10^1
Transaction Count

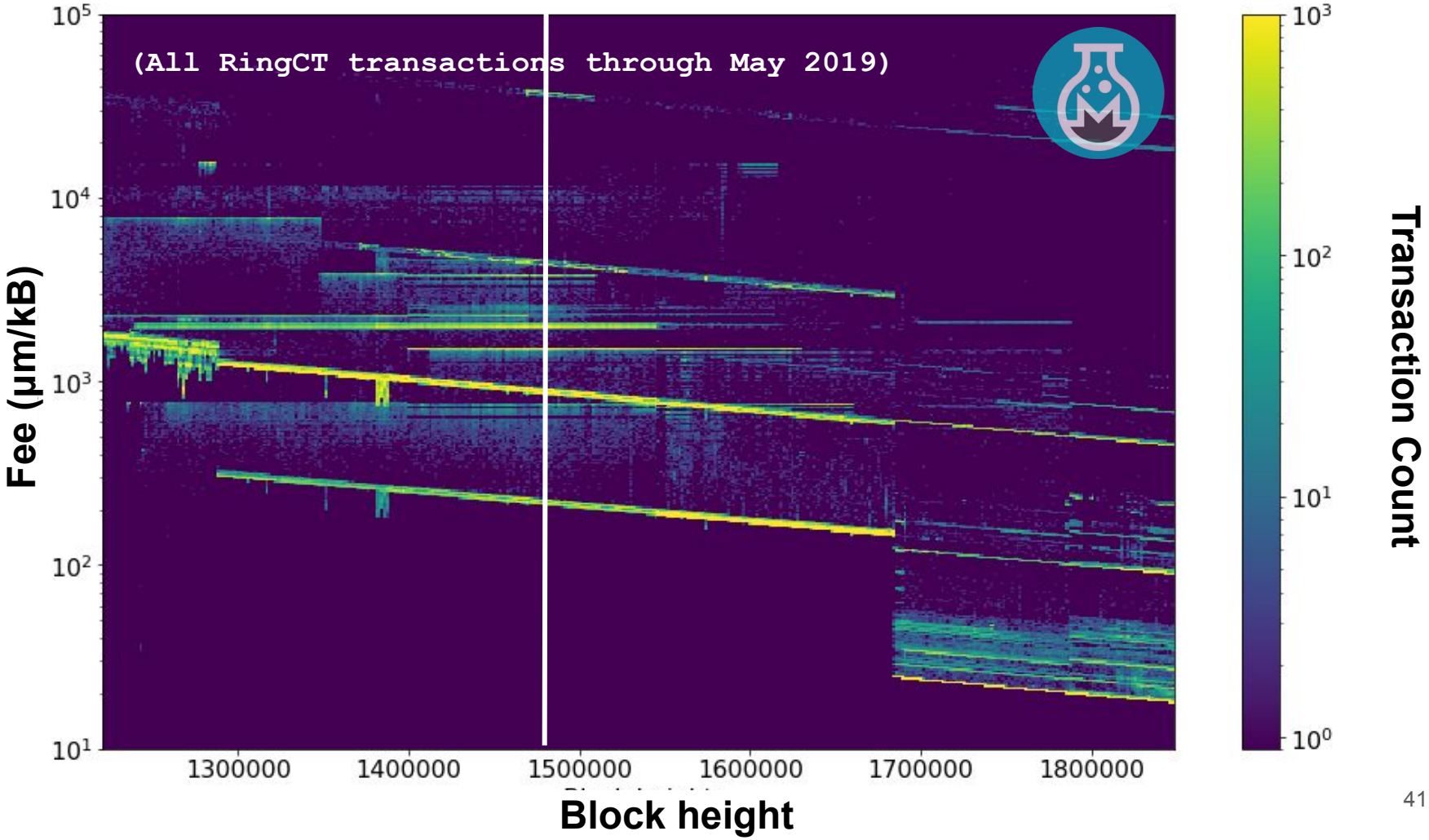

(All RingCT transactions through May 2019)
Some of this fanning due to different-sized transactions
Fee (μm)
10^5
10^4
10^3
10^2
10^1
1300000
1400000
1500000
1600000
1700000
1800000
Block height
Transaction Count
10^4
10^3
10^2
10^1

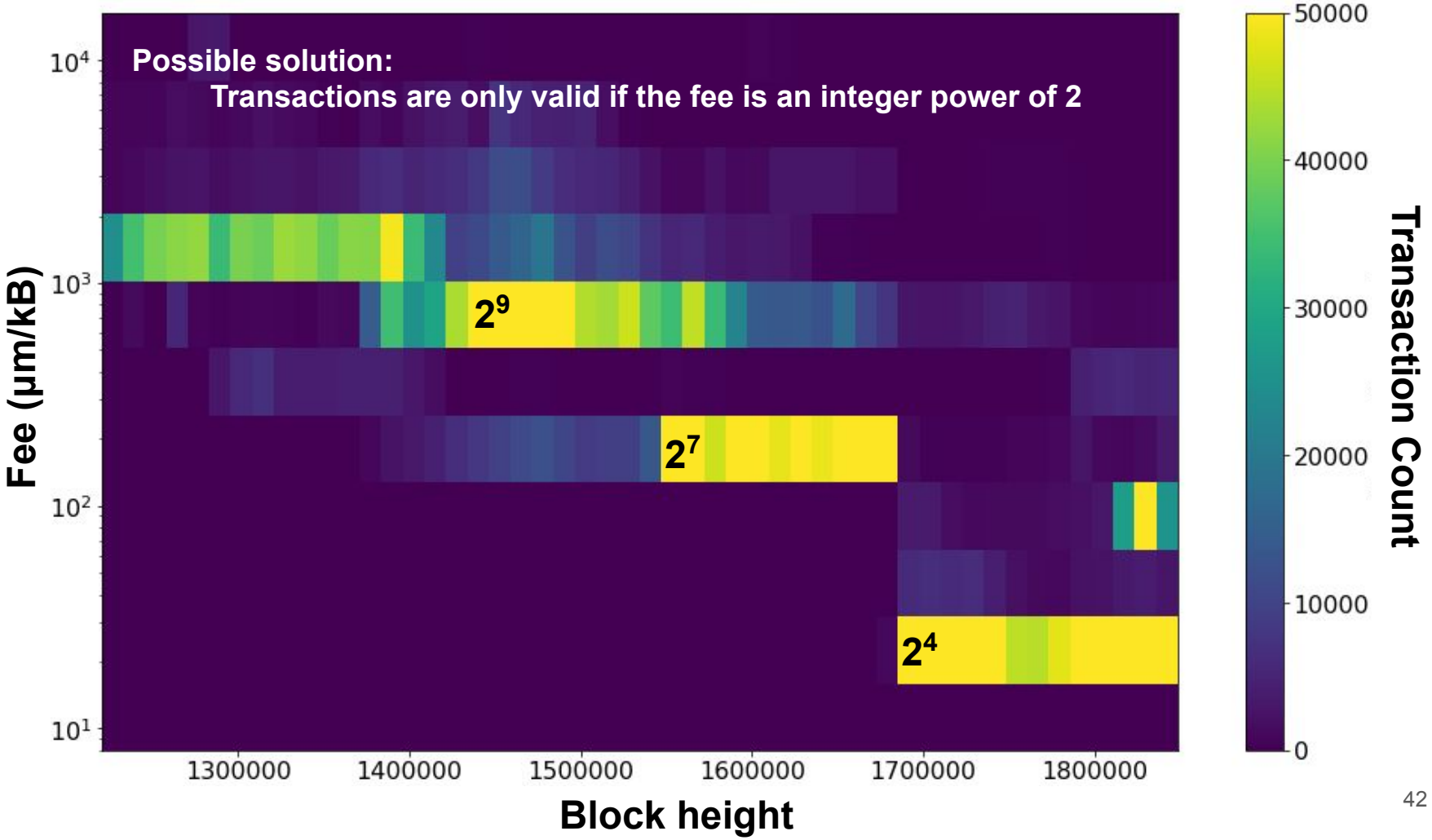

(All RingCT transactions through May 2019)
Fee (µm/kB)
10^5
10^4
10^3
10^2
10^1
1300000
1400000
1500000
1600000
1700000
1800000
Block height
10^3
10^2
10^1
10^0
Transaction Count

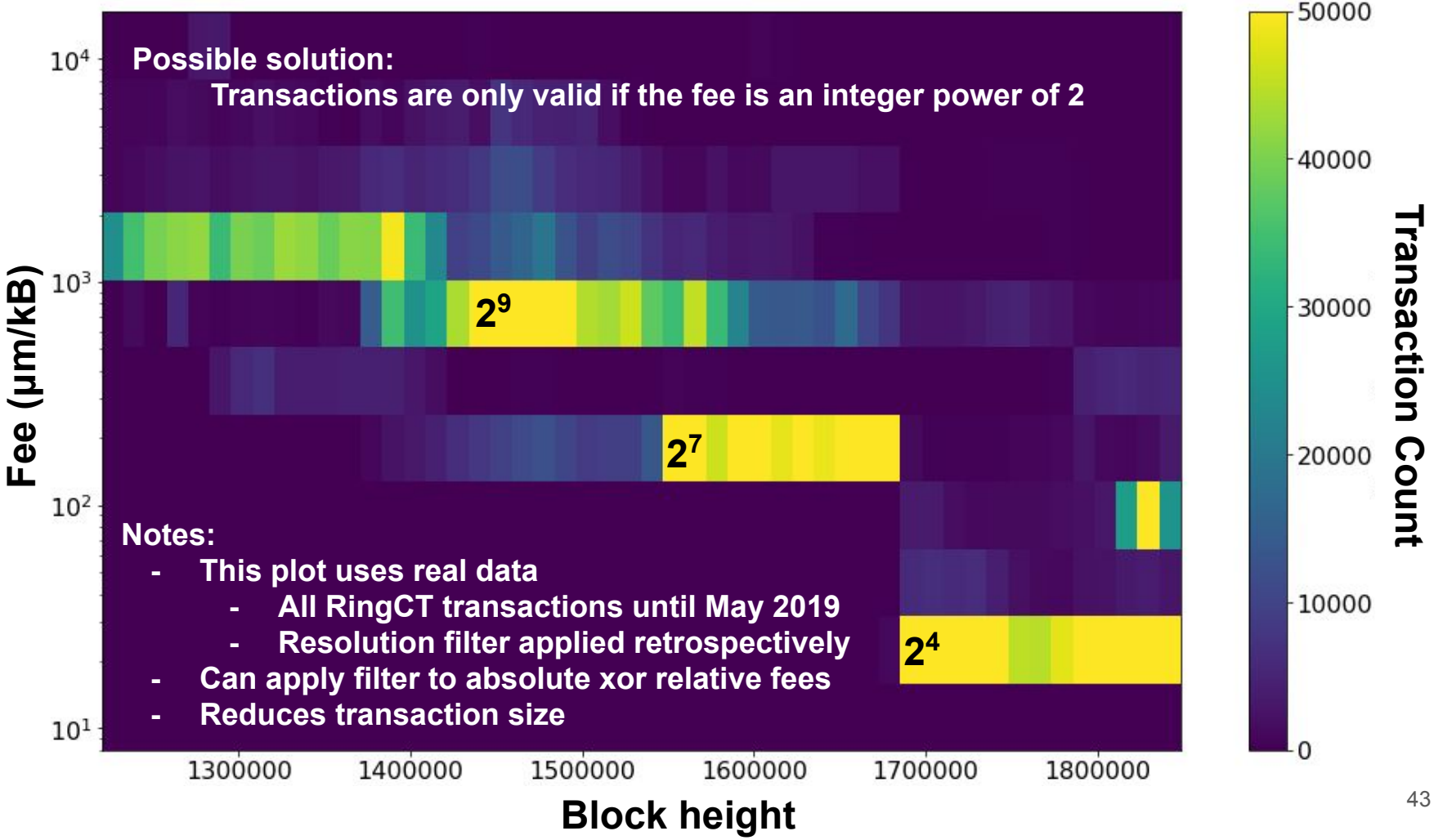

(All RingCT transactions through May 2019)
Fee (µm/kB)
10^5
10^4
10^3
10^2
10^1
1300000
1400000
1500000
1600000
1700000
1800000
Block height
Different priority levels
10^3
10^2
10^1
10^0
Transaction Count


(All RingCT transactions through May 2019)
Fee (µm/kB)
10^5
10^4
10^3
10^2
10^1
1300000
1400000
1500000
1600000
1700000
1800000
Block height
Different priority levels
Fee sniping?
10^3
10^2
10^1
10^0
Transaction Count


(All RingCT transactions through May 2019)
Fee exactly
1530.338970 um/kB
Anonymity puddle:
22k out of 3700k
(~0.6%)
Fee (µm/kB)
Block height
Transaction Count
10^5
10^4
10^3
10^2
10^1
1300000
1400000
1500000
1600000
1700000
1800000
10^3
10^2
10^1
10^0


(All RingCT transactions through May 2019)
Fee (µm/kB)
10^5
10^4
10^3
10^2
10^1
1300000
1400000
1500000
1600000
1700000
1800000
Block height
10^3
10^2
10^1
10^0
Transaction Count


Possible solution:
Transactions are only valid if the fee is an integer power of 2
2^9
2^7
2^4
Fee (µm/kB)
10^4
10^3
10^2
10^1
1300000
1400000
1500000
1600000
1700000
1800000
Block height
50000
40000
30000
20000
10000
0
Transaction Count


Possible solution:
Transactions are only valid if the fee is an integer power of 2
2^9
2^7
2^4
Notes:
- This plot uses real data
  - All RingCT transactions until May 2019
  - Resolution filter applied retrospectively
- Can apply filter to absolute xor relative fees
- Reduces transaction size
Fee (µm/kB)
10^4
10^3
10^2
10^1
1300000
1400000
1500000
1600000
1700000
1800000
Block height
50000
40000
30000
20000
10000
0
Transaction Count

Act I conclusions:

- >= Four separate anonymity pools
  - Correct (reference) dynamic fee algorithm
    - Example: priority level = {1,2,3,4}

Act I conclusions:

- >= Four separate anonymity pools
  - Correct (reference) dynamic fee algorithm
    - Example: priority level = {1,2,3,4}
  - Fixed absolute fee
    - Example: fee always 0.002 XMR

Act I conclusions:

- >= Four separate anonymity pools
  - Correct (reference) dynamic fee algorithm
    - Example: priority level = {1,2,3,4}
  - Fixed absolute fee
    - Example: fee always 0.002 XMR
  - Fixed fee per weight
    - Example: fee always 0.01 XMR / kB

Act I conclusions:

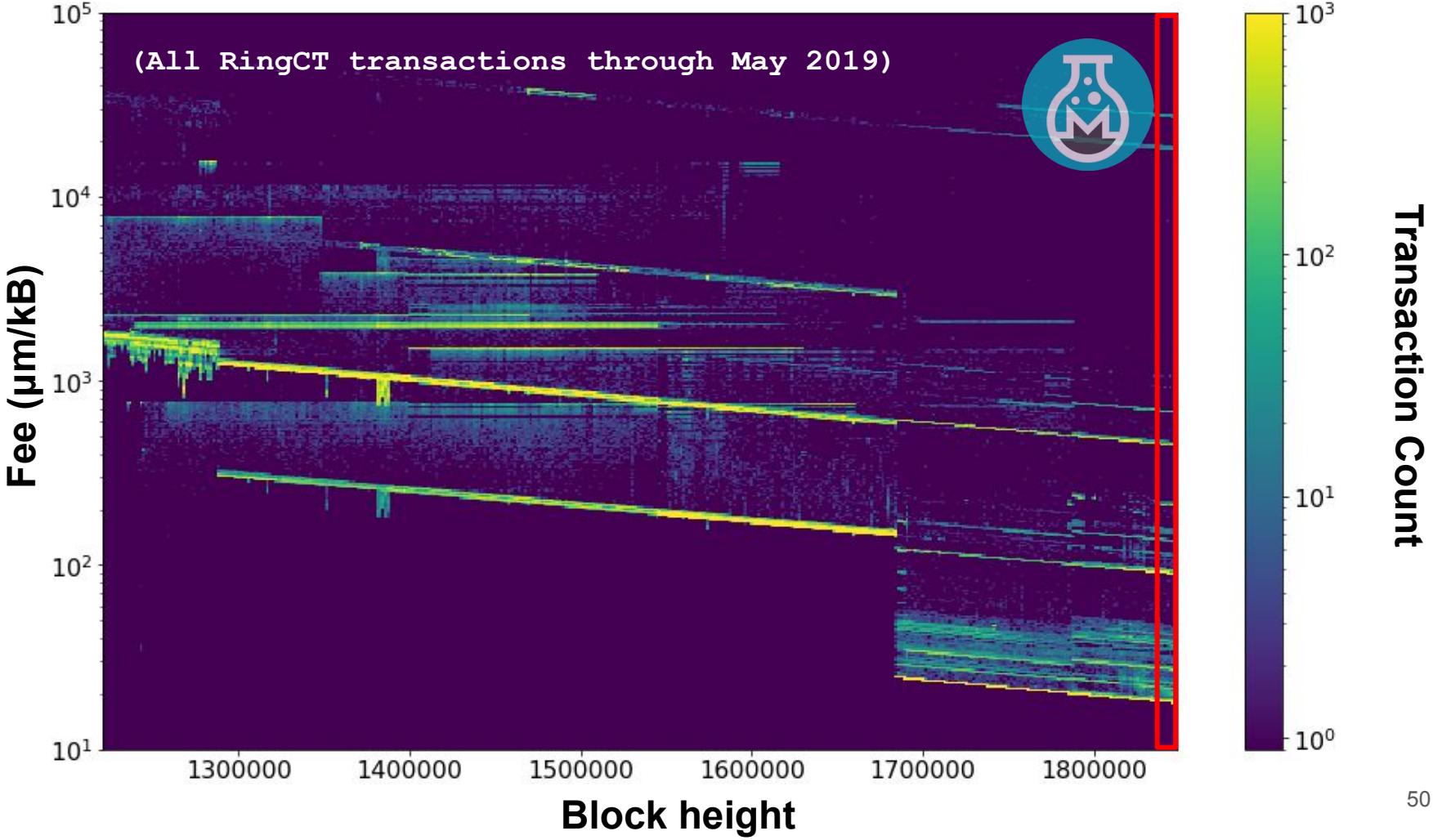
- >= Four separate anonymity pools
  - Correct (reference) dynamic fee algorithm
    - Example: priority level = {1,2,3,4}
  - Fixed absolute fee
    - Example: fee always 0.002 XMR
  - Fixed fee per weight
    - Example: fee always 0.01 XMR / kB
  - Outliers to above 3 sets

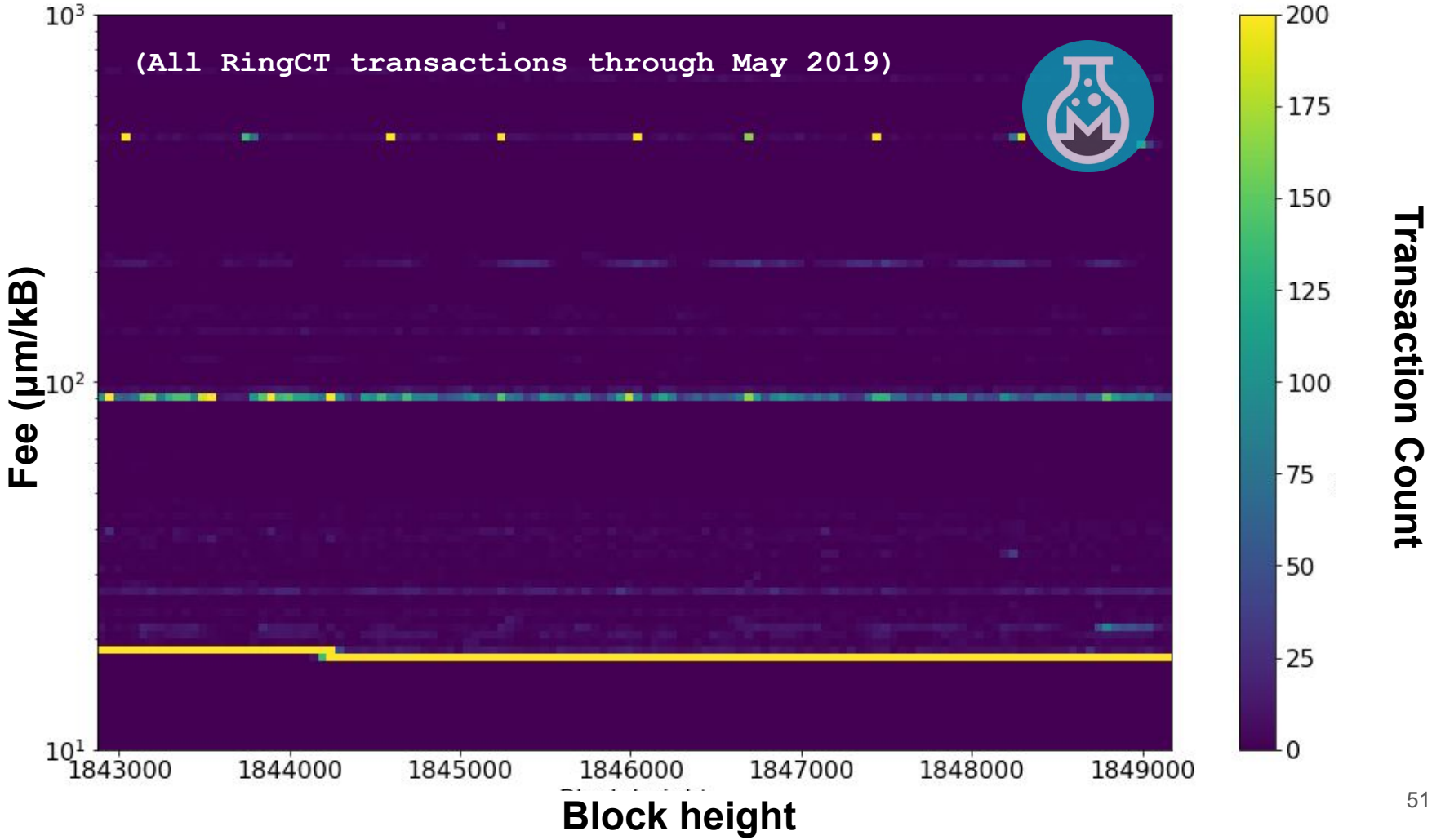
Act I conclusions:

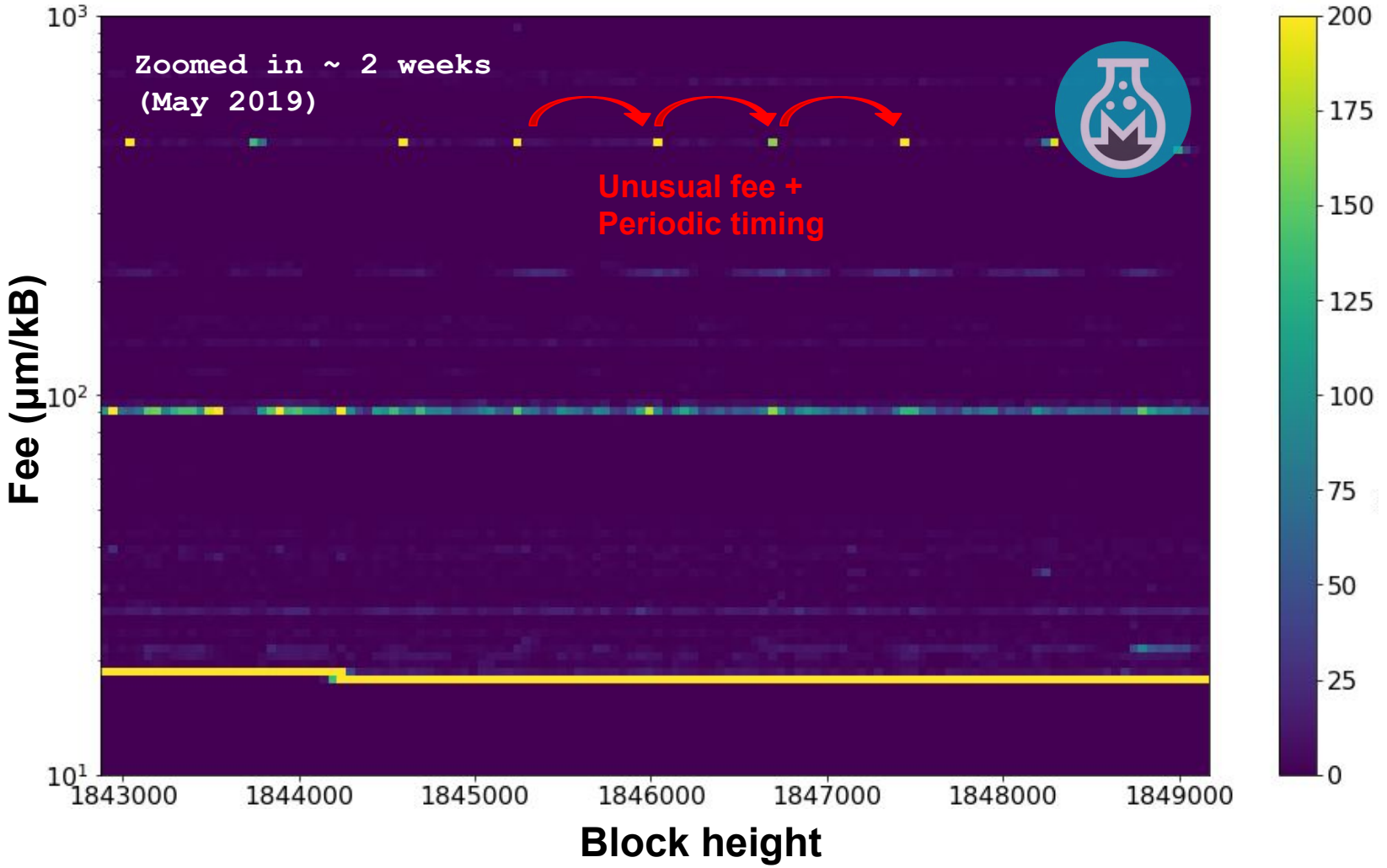
- >= Four separate anonymity pools
  - Correct (reference) dynamic fee algorithm
    - Example: priority level = {1,2,3,4}
  - Fixed absolute fee
    - Example: fee always 0.002 XMR
  - Fixed fee per weight
    - Example: fee always 0.01 XMR / kB
  - Outliers to above 3 sets
- Recommend eliminating high precision fees
  - Example: 1030.338970 um/kB → 2^10

Act I conclusions:

- >= Four separate anonymity pools
  - Correct (reference) dynamic fee algorithm
    - Example: priority level = {1,2,3,4}
  - Fixed absolute fee
    - Example: fee always 0.002 XMR
  - Fixed fee per weight
    - Example: fee always 0.01 XMR / kB
  - Outliers to above 3 sets
- Recommend eliminating high precision fees
  - Example: 1030.338970 um/kB → 2^10
- Fee fingerprinting can be combined with other heuristics
  - Example: timing analysis


(All RingCT transactions through May 2019)
Fee (µm/kB)
10^5
10^4
10^3
10^2
10^1
1300000
1400000
1500000
1600000
1700000
1800000
Block height
10^3
10^2
10^1
10^0
Transaction Count

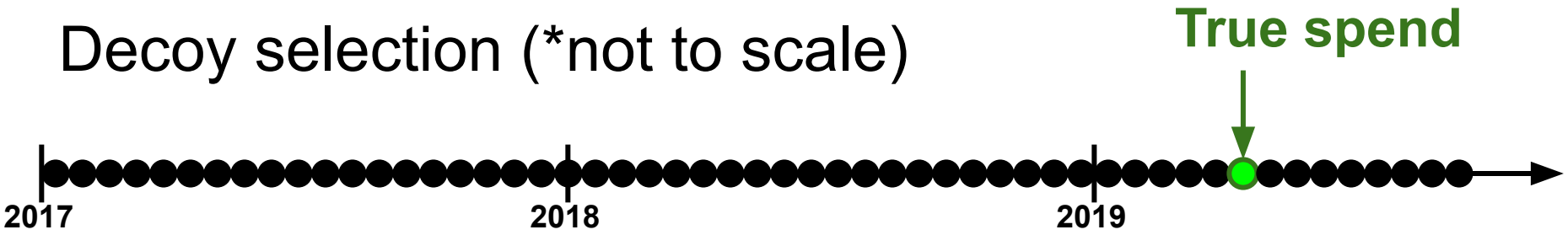

(All RingCT transactions through May 2019)
Fee (µm/kB)
10^3
10^2
10^1
1843000
1844000
1845000
1846000
1847000
1848000
1849000
Block height
200
175
150
125
100
75
50
25
0
Transaction Count


Zoomed in ~ 2 weeks
(May 2019)
Unusual fee +
Periodic timing
10^3
10^2
10^1
Fee (µm/kB)
1843000
1844000
1845000
1846000
1847000
1848000
1849000
Block height
200
175
150
125
100
75
50
25
0
Transaction Count

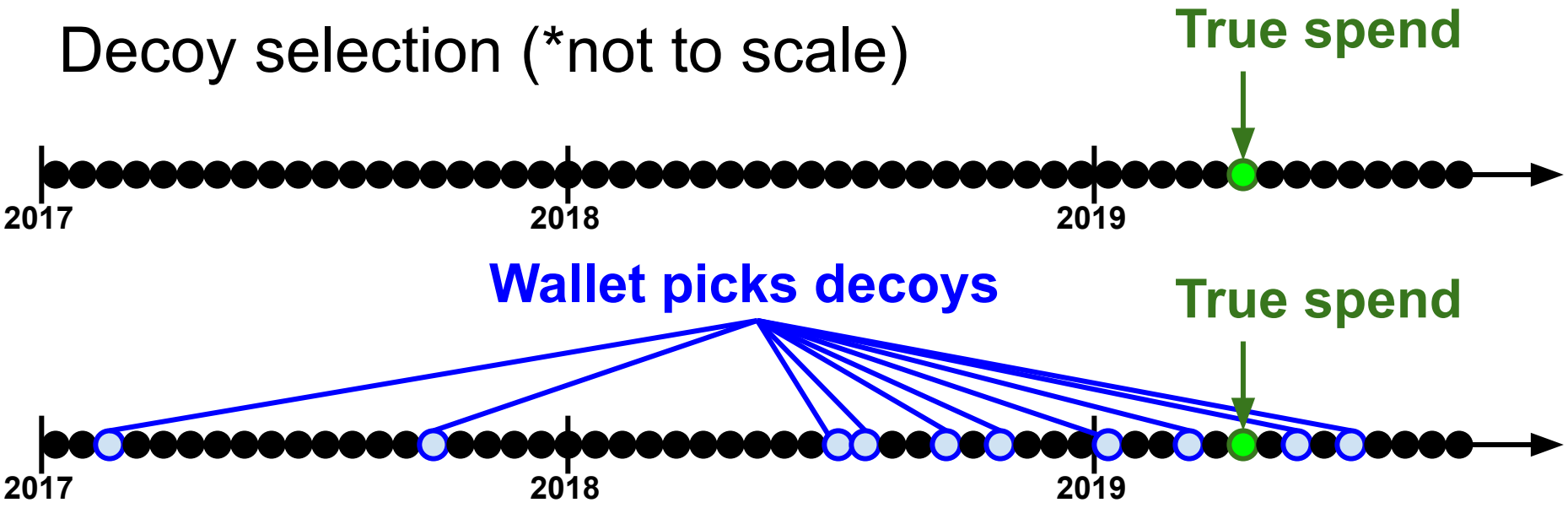
Act II

Juvenile ring members

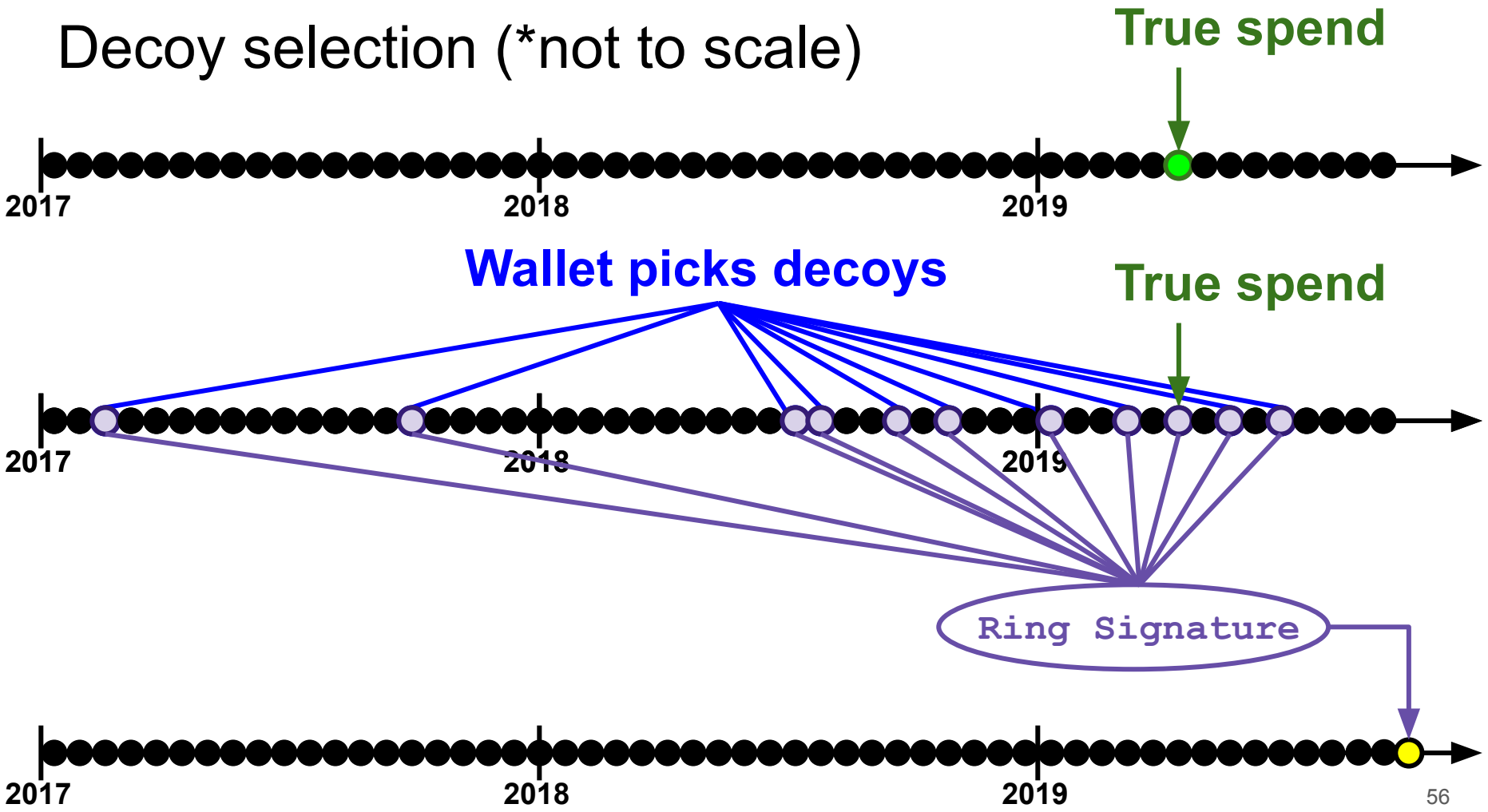
Decoy selection (*not to scale)



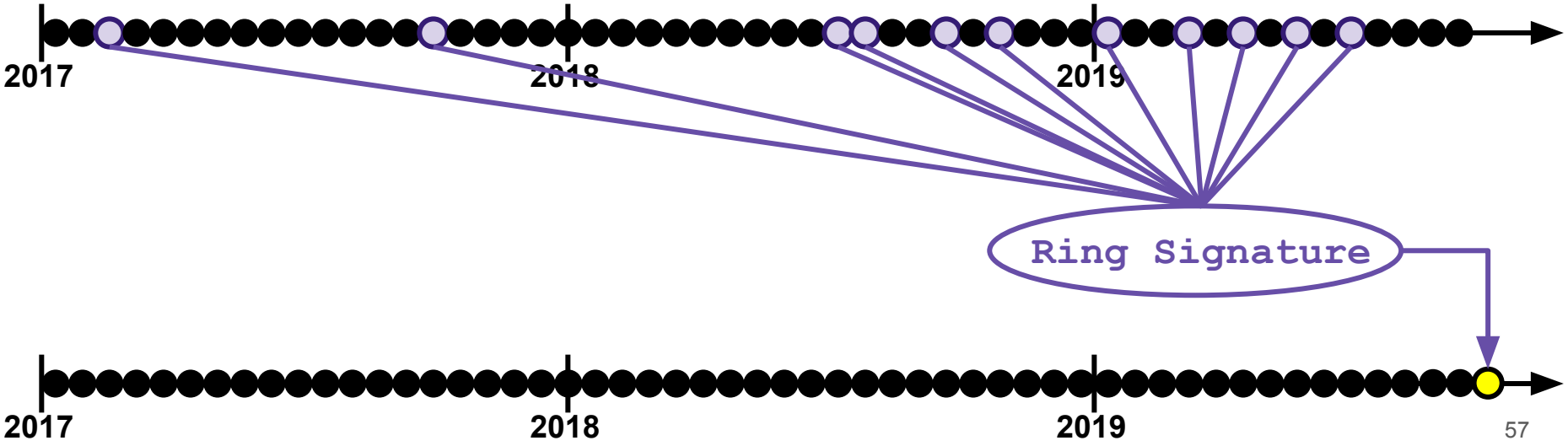
Decoy selection (*not to scale)



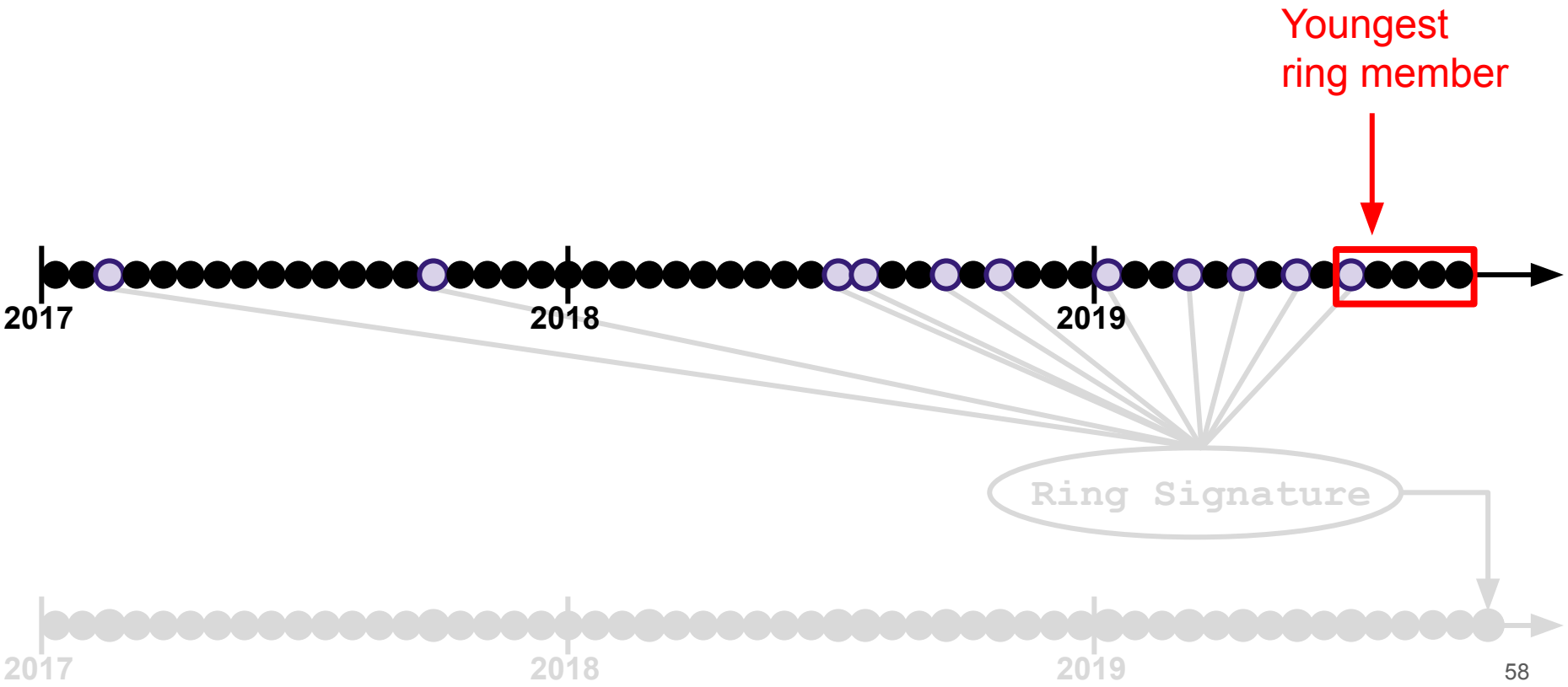
Decoy selection (*not to scale)



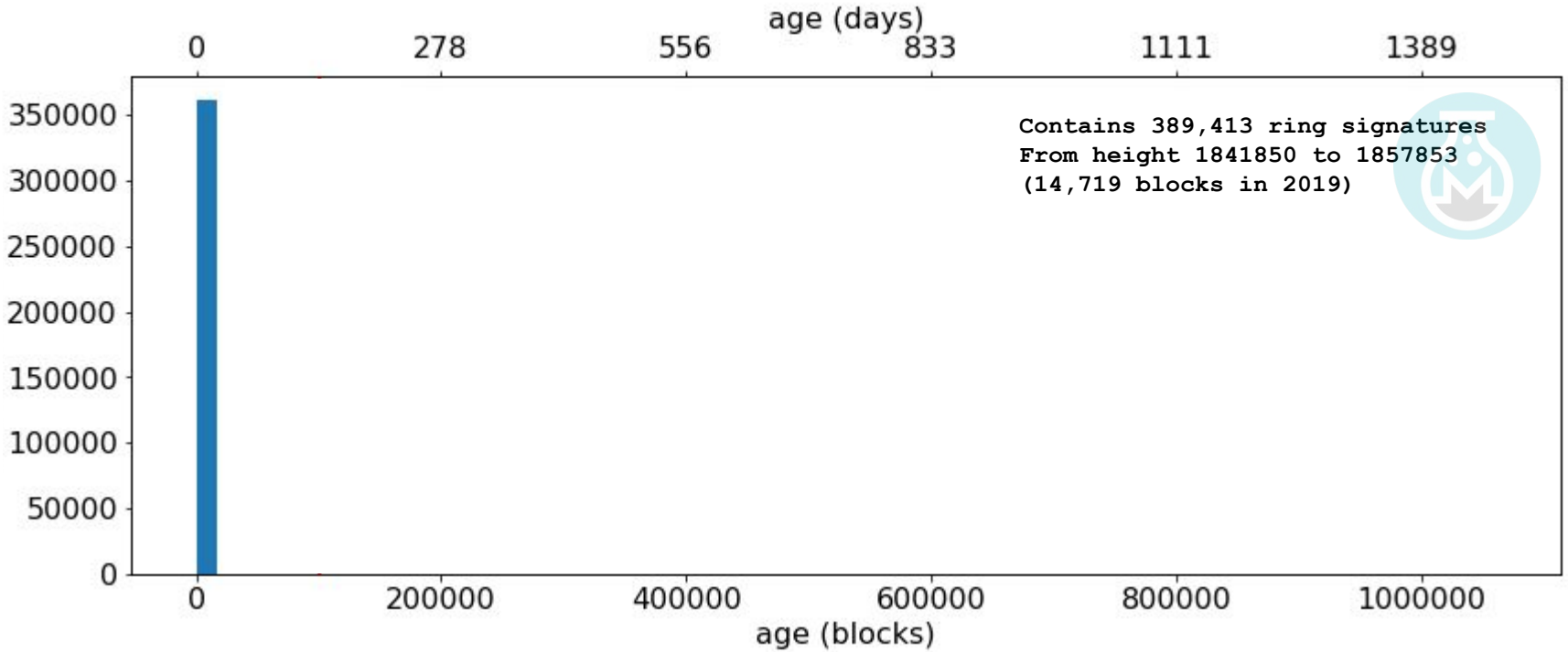
This is what outside observers see:



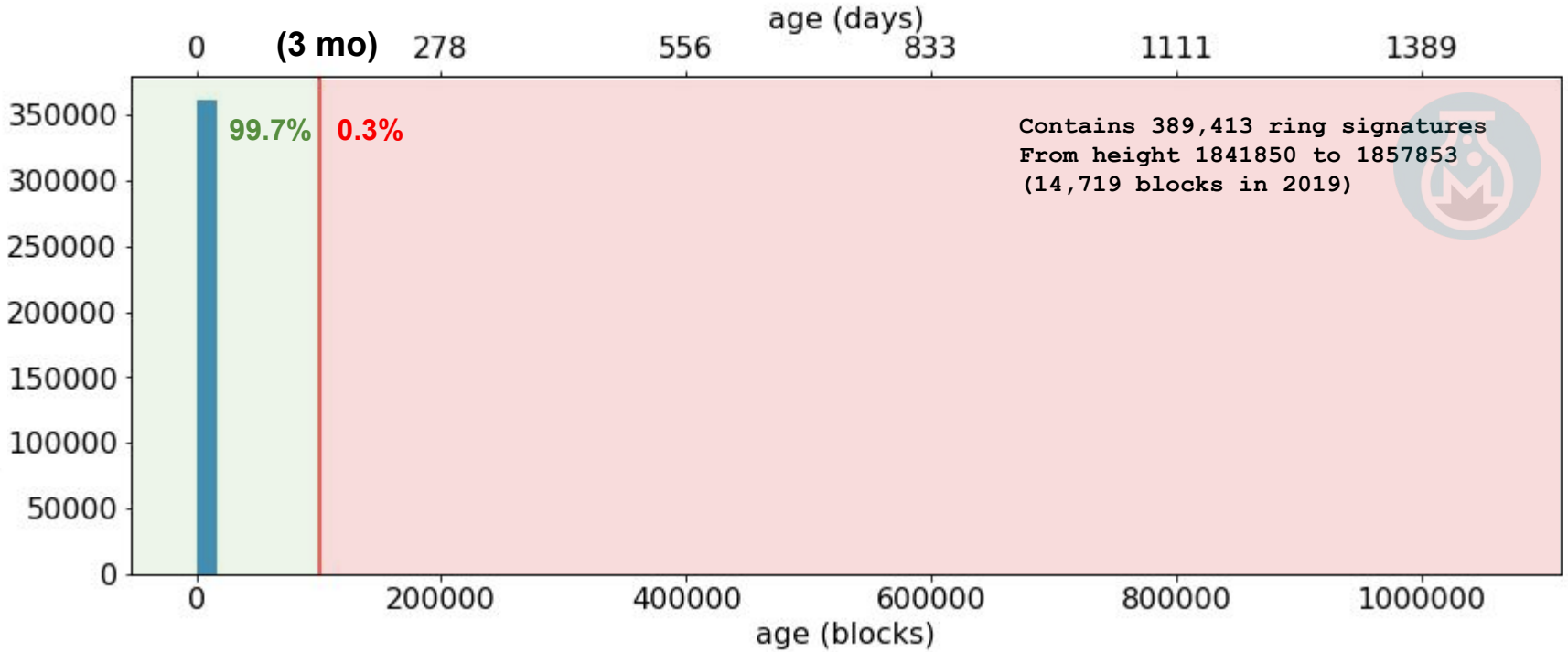
This is what outside observers can analyze:



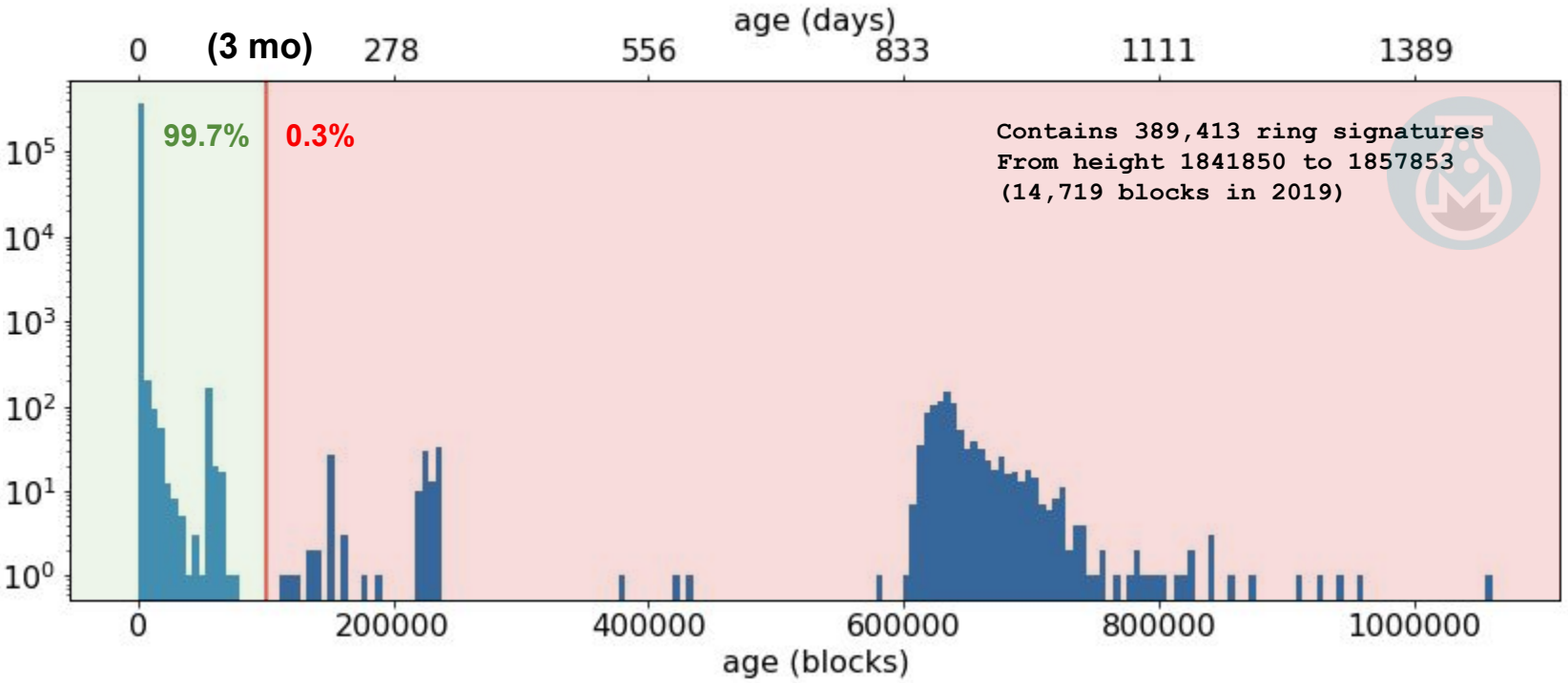
Youngest ring member



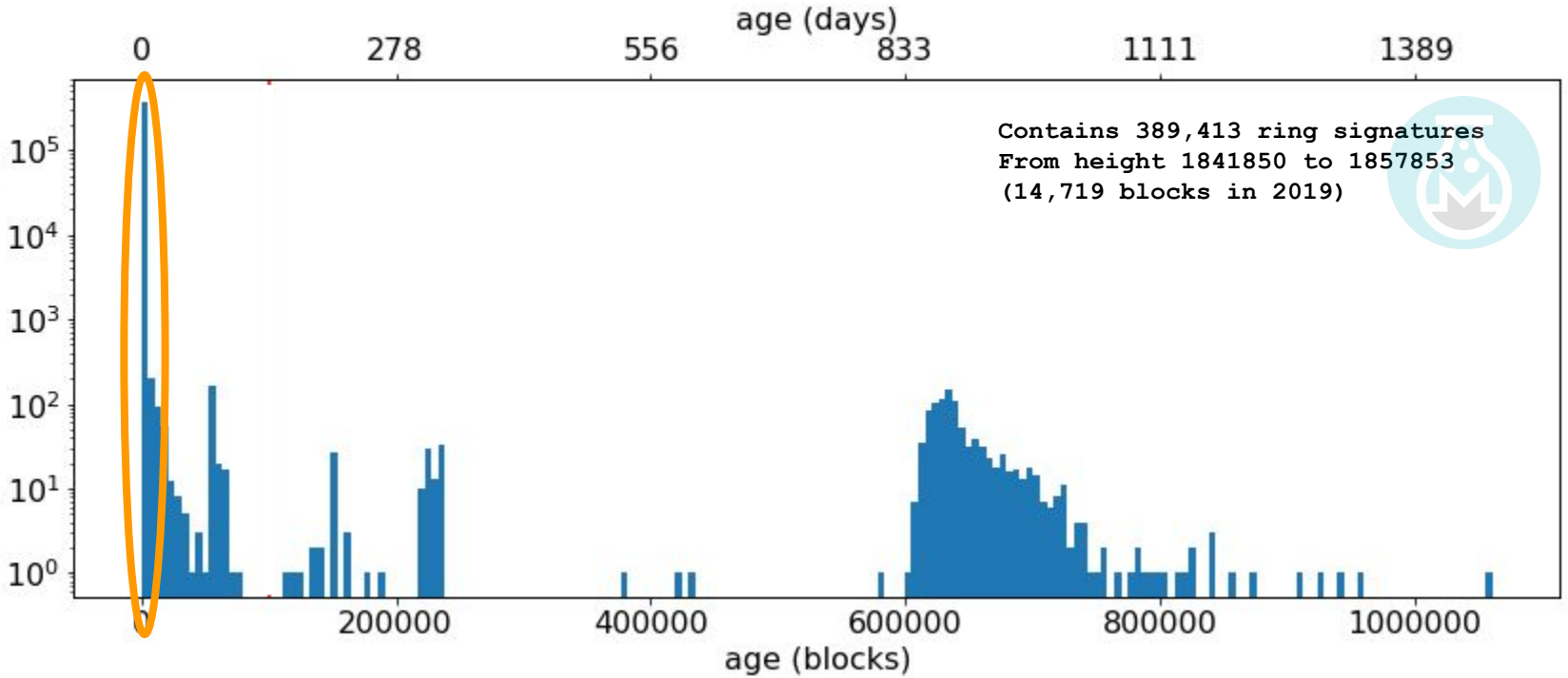
Youngest ring member



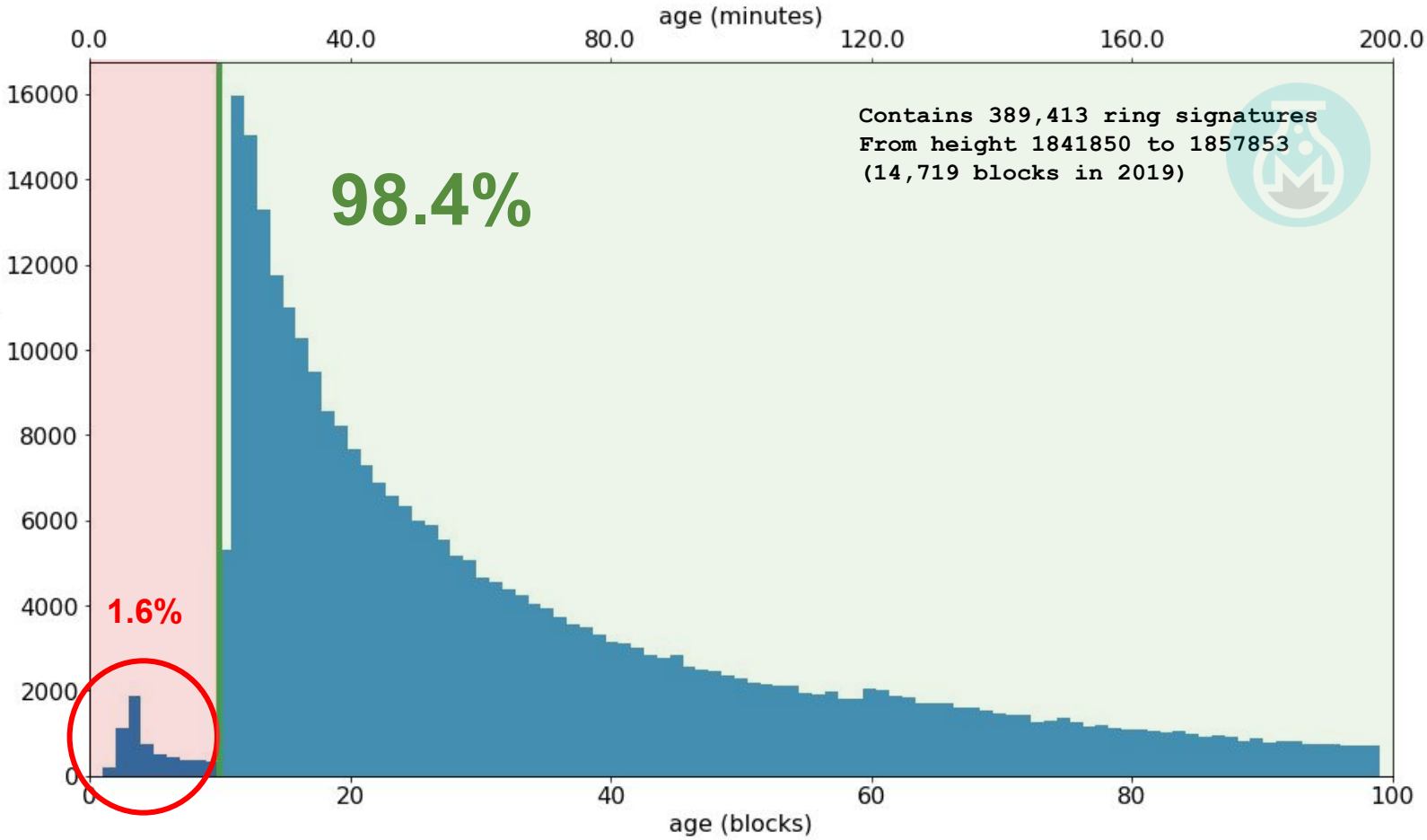
Youngest ring member

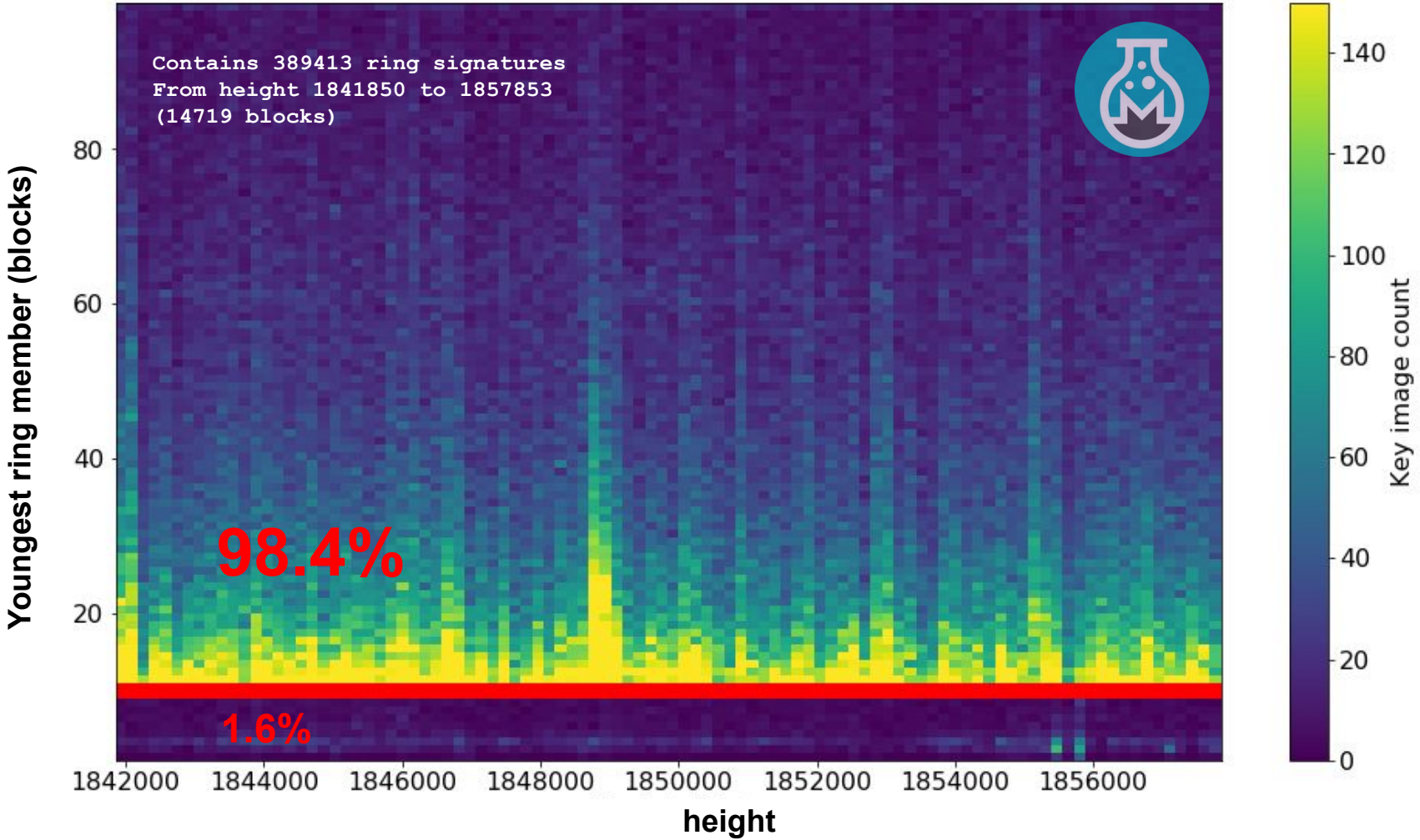


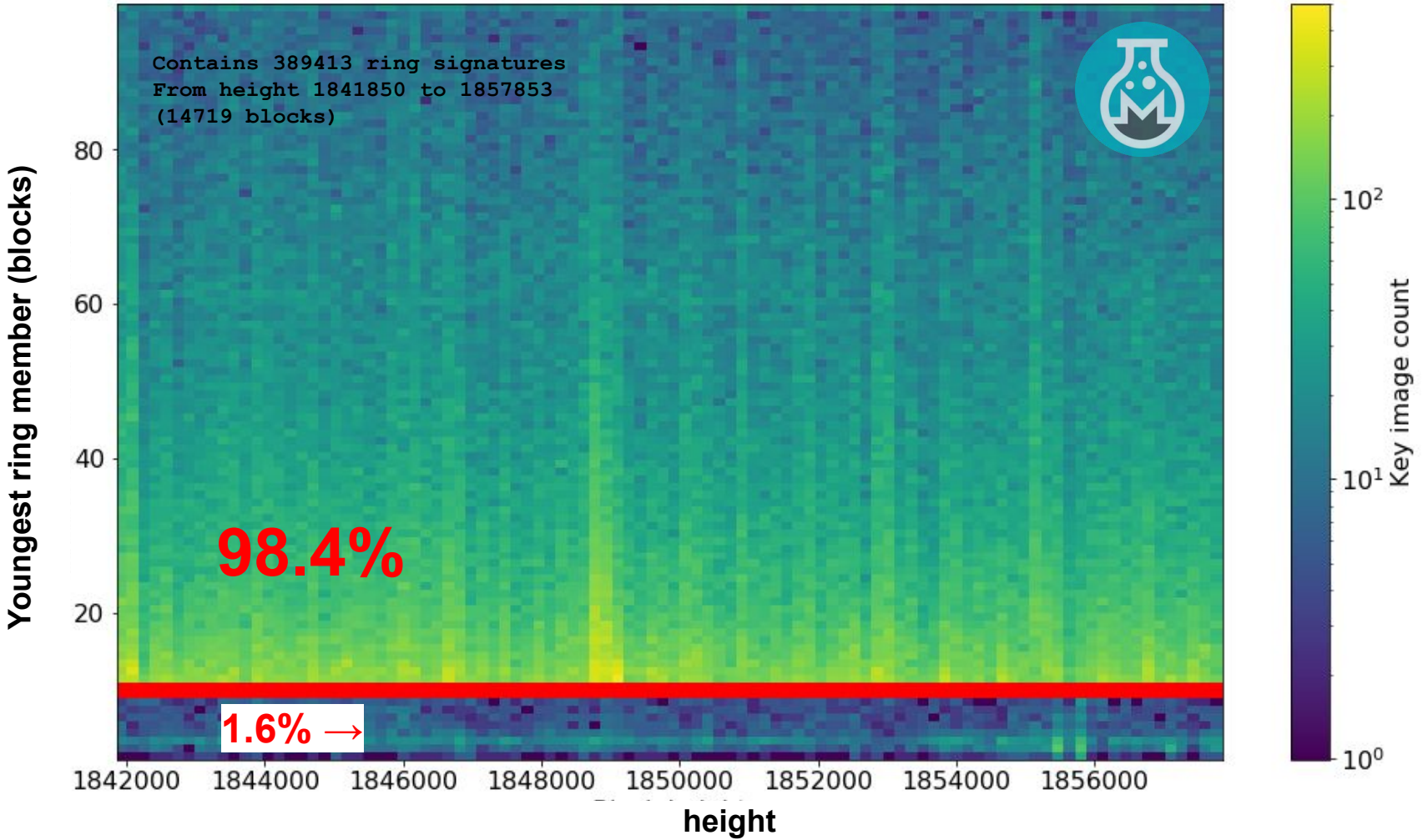
Youngest ring member



Youngest ring member (zoomed in)




Contains 389413 ring signatures
From height 1841850 to 1857853
(14719 blocks)
98.4%
1.6%
Youngest ring member (blocks)
height
Key image count
80
60
40
20
1842000
1844000
1846000
1848000
1850000
1852000
1854000
1856000
140
120
100
80
60
40
20
0


Contains 389413 ring signatures
From height 1841850 to 1857853
(14719 blocks)
98.4%
1.6% →
Youngest ring member (blocks)
80
60
40
20
1842000
1844000
1846000
1848000
1850000
1852000
1854000
1856000
height
10^2
10^1
10^0
Key image count

Act II Conclusions:

- **Vast majority (98.4%) of anonymity pool follows 10 block lock time**
- **Minority (1.6%) of ring signatures include members less than 10 blocks old**

Act II Conclusions:

- Vast majority (98.4%) of anonymity pool follows 10 block lock time
- Minority (1.6%) of ring signatures include members less than 10 blocks old
- Protocol should enforce (privacy-relevant) reference wallet rules

Act II Conclusions:

- Vast majority (98.4%) of anonymity pool follows 10 block lock time
- Minority (1.6%) of ring signatures include members less than 10 blocks old
- Protocol should enforce (privacy-relevant) reference wallet rules
- Options:
  1. Impose 10-block lock at protocol level
  2. Remove 10-block lock in reference wallet
  3. Compromise (lesser lock time implemented protocol)

Act II Conclusions:

- Vast majority (98.4%) of anonymity pool follows 10 block lock time
- Minority (1.6%) of ring signatures include members less than 10 blocks old
- Protocol should enforce (privacy-relevant) reference wallet rules
- Options:
  1. Impose 10-block lock at protocol level
  2. Remove 10-block lock in reference wallet
  3. Compromise (lesser lock time implemented protocol)
- I currently prefer #1 until / unless research suggests < 10 is safe
- Note: this is unrelated to buyers permitting 0-confirmation purchases

Act II Conclusions:

- Vast majority (98.4%) of anonymity pool follows 10 block lock time
- Minority (1.6%) of ring signatures include members less than 10 blocks old
- Protocol should enforce (privacy-relevant) reference wallet rules
- Options:
  1. Impose 10-block lock at protocol level
  2. Remove 10-block lock in reference wallet
  3. Compromise (lesser lock time implemented protocol)
- I currently prefer #1 until / unless research suggests < 10 is safe
- Note: this is unrelated to buyers permitting 0-confirmation purchases
- AFAIK 10 blocks was chosen arbitrarily, is this optimal? *(Out of scope)*

Act III

Egregious decoy selection

Standard (= best practices) decoy selection:

2016 **today**

***Not to scale**

Standard (= best practices) decoy selection:

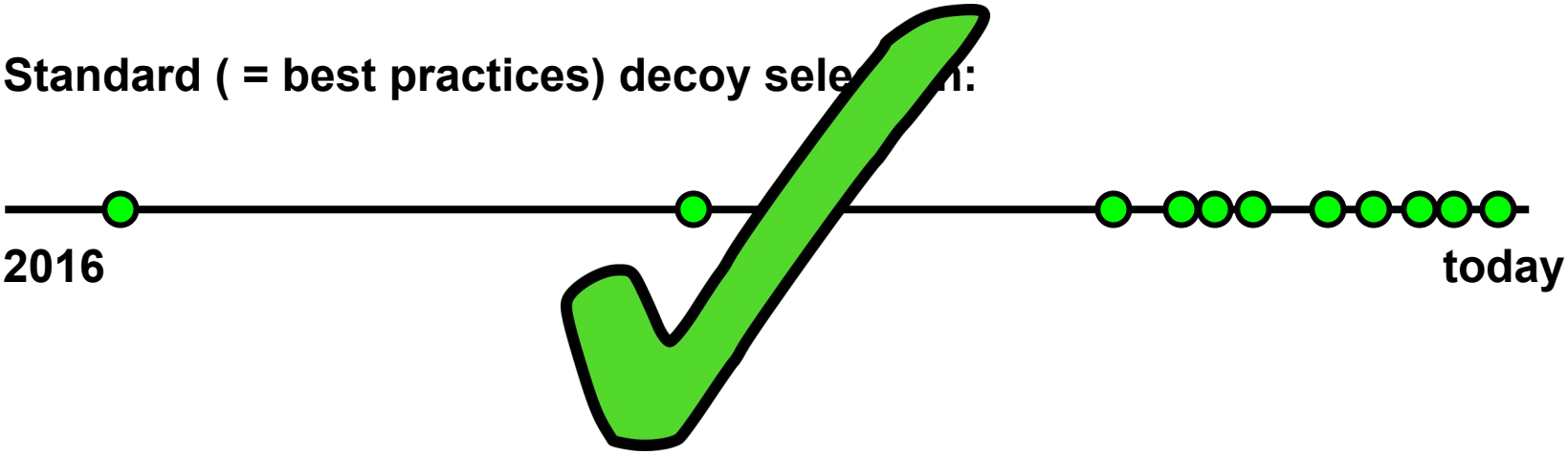
2016 **today**

Uniform random (= bad practice) decoy selection:

2016 **today**

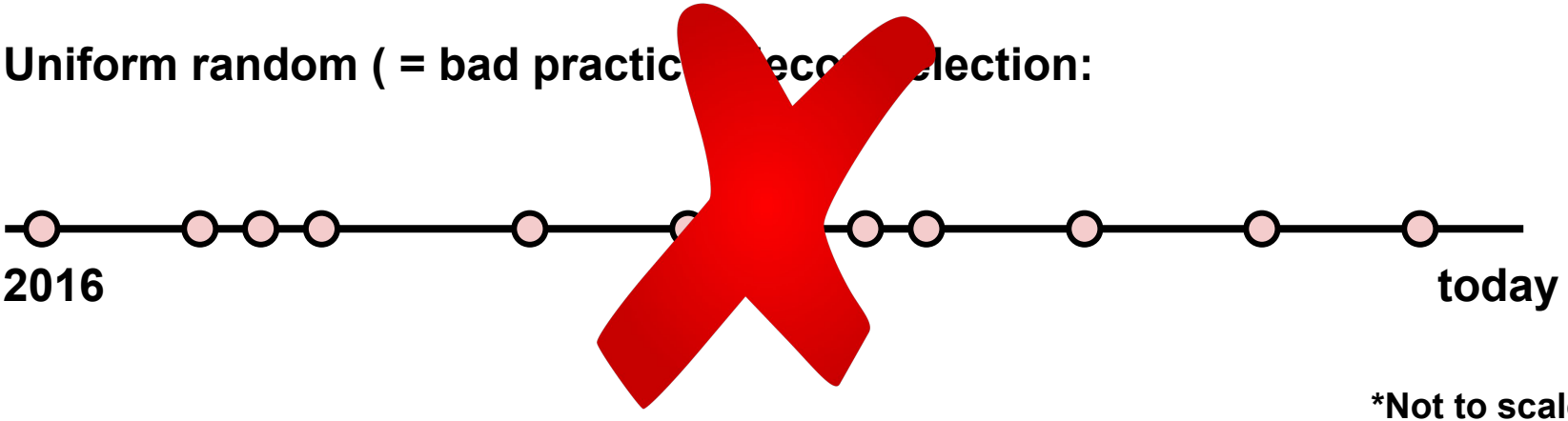
***Not to scale**

Standard (= best practices) decoy sele n:



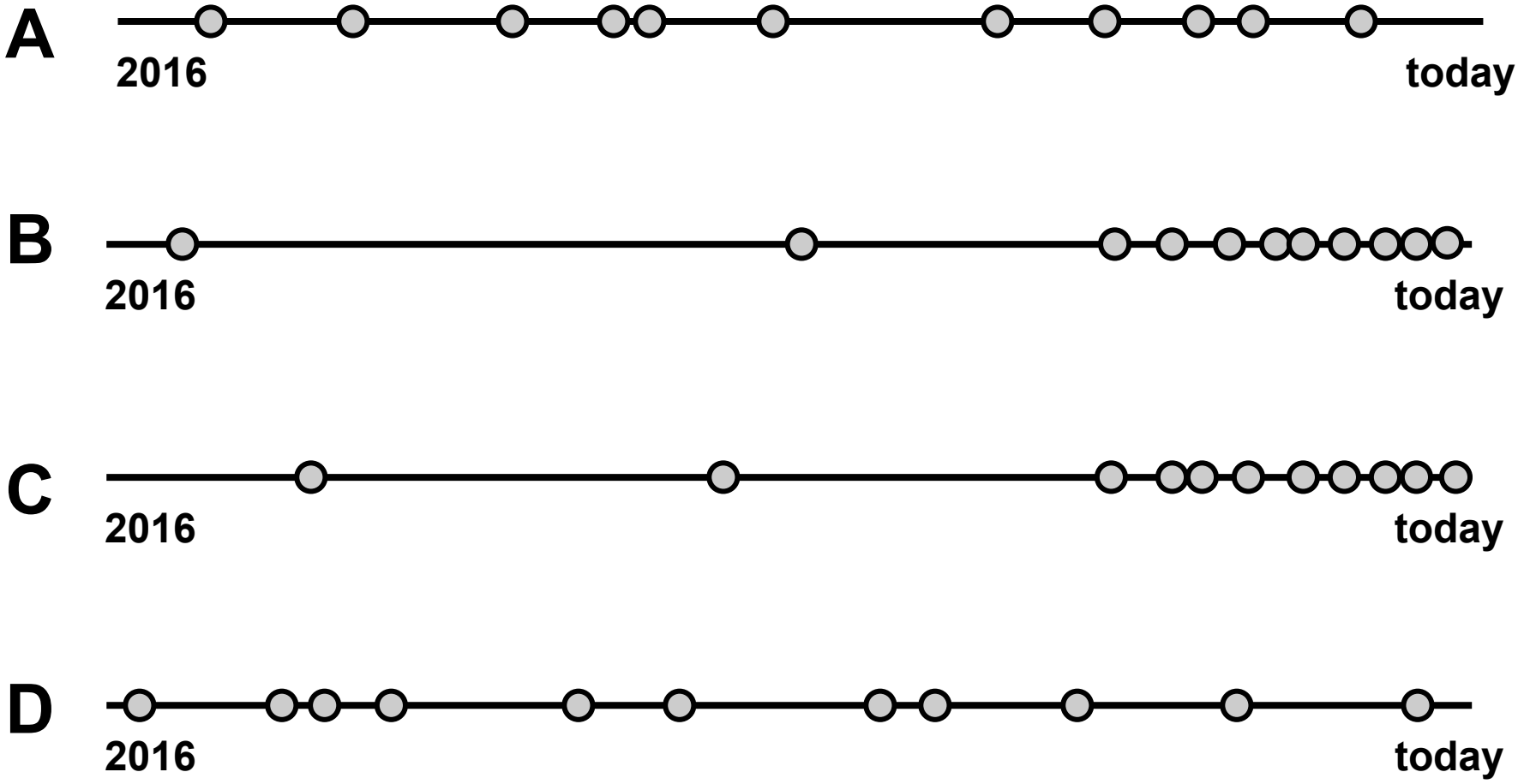
2016 **today**

Uniform random (= bad practic ecoy lection:

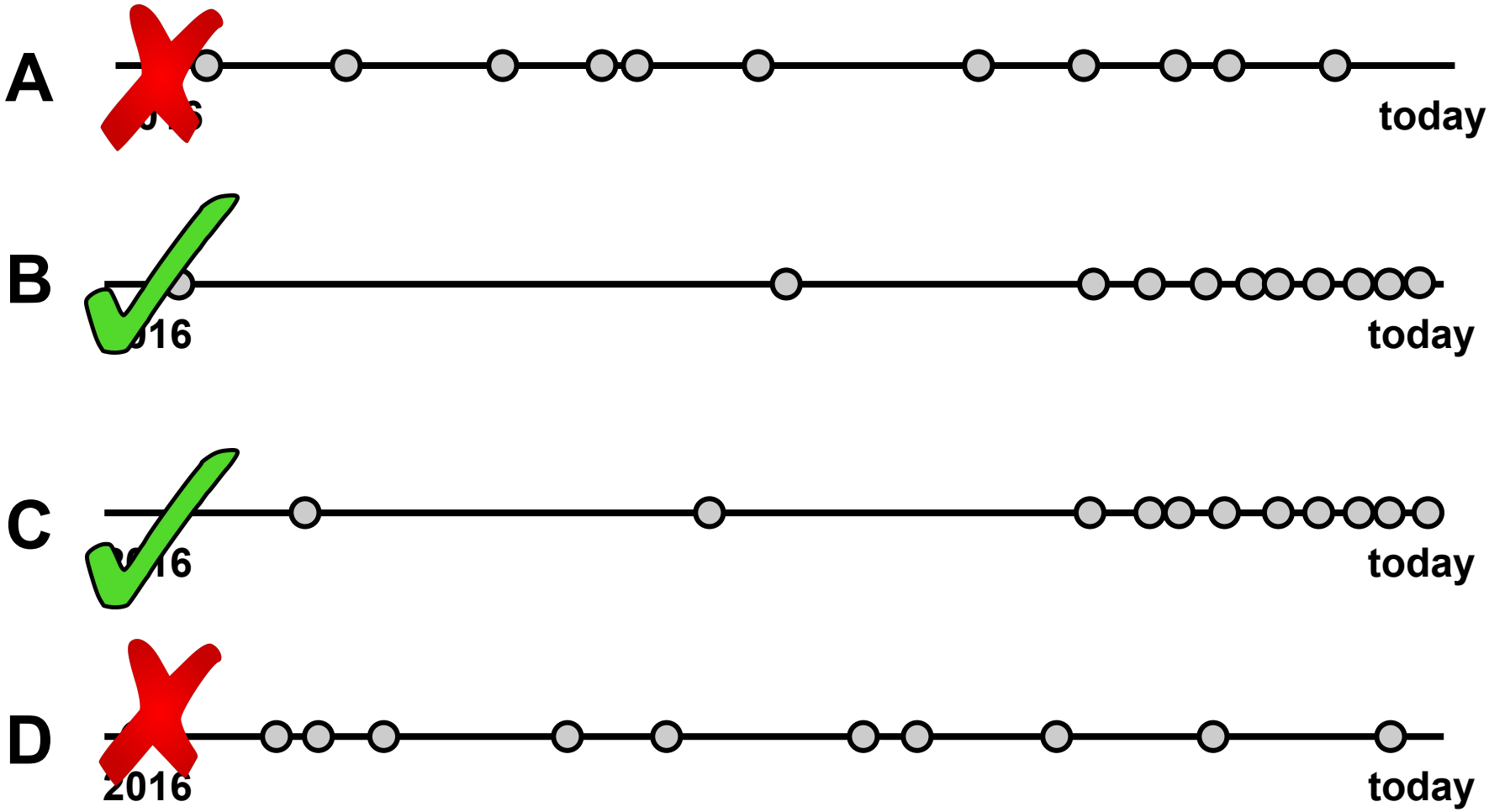


2016 **today**

***Not to scale**

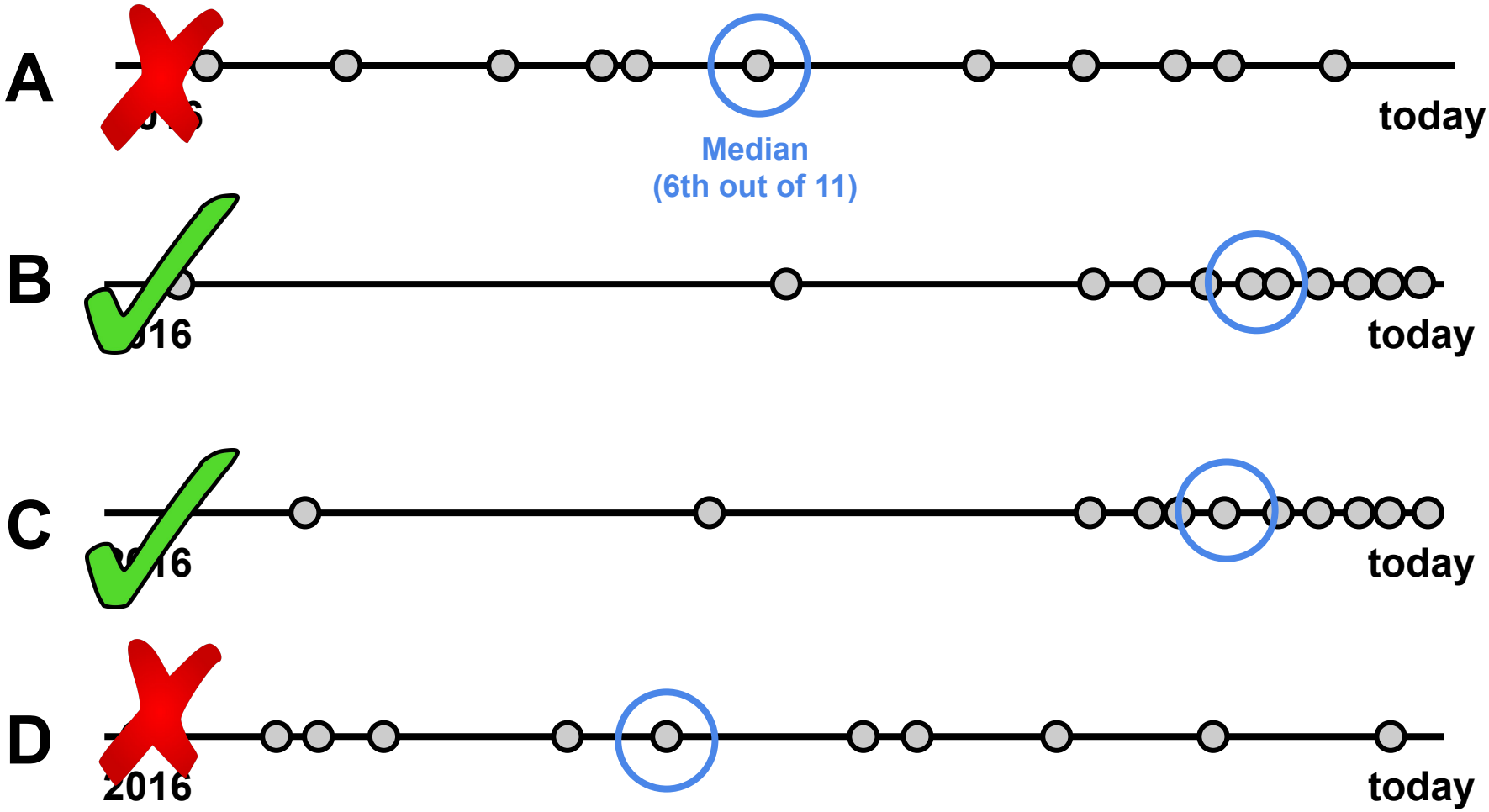


*Not to scale



Non-deterministic =/= non-verifiable

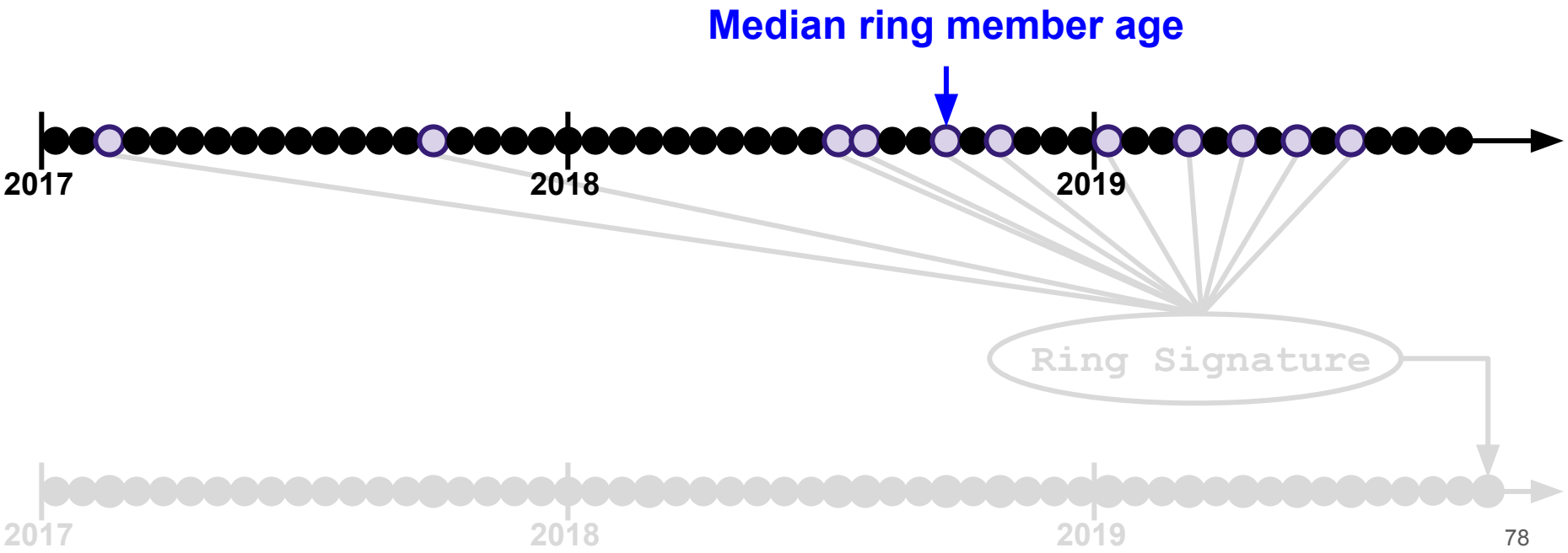
*Not to scale



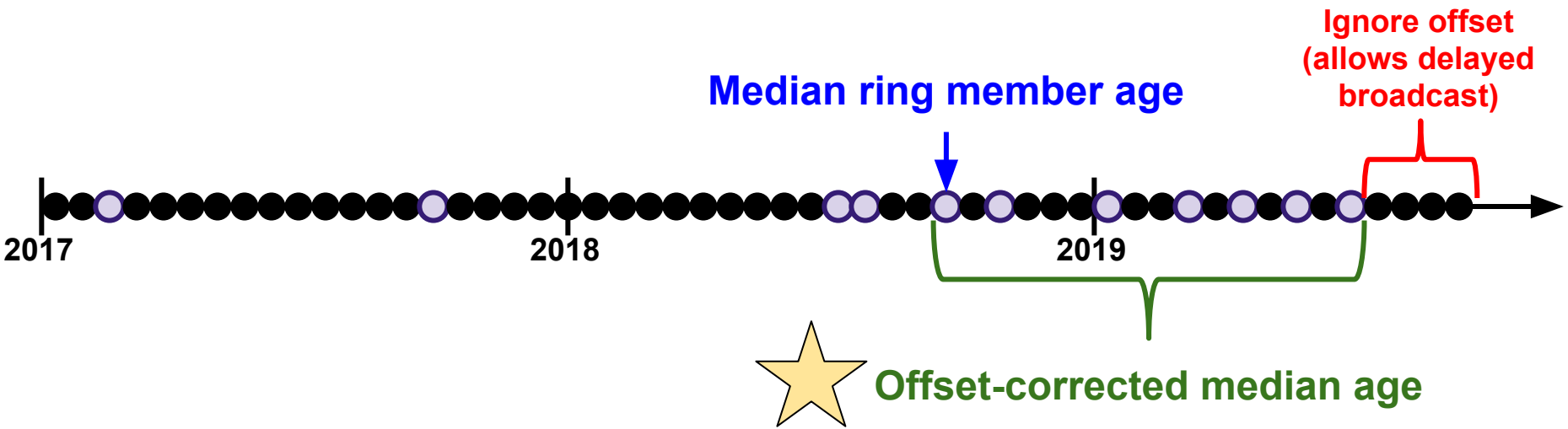
Non-deterministic =/= non-verifiable

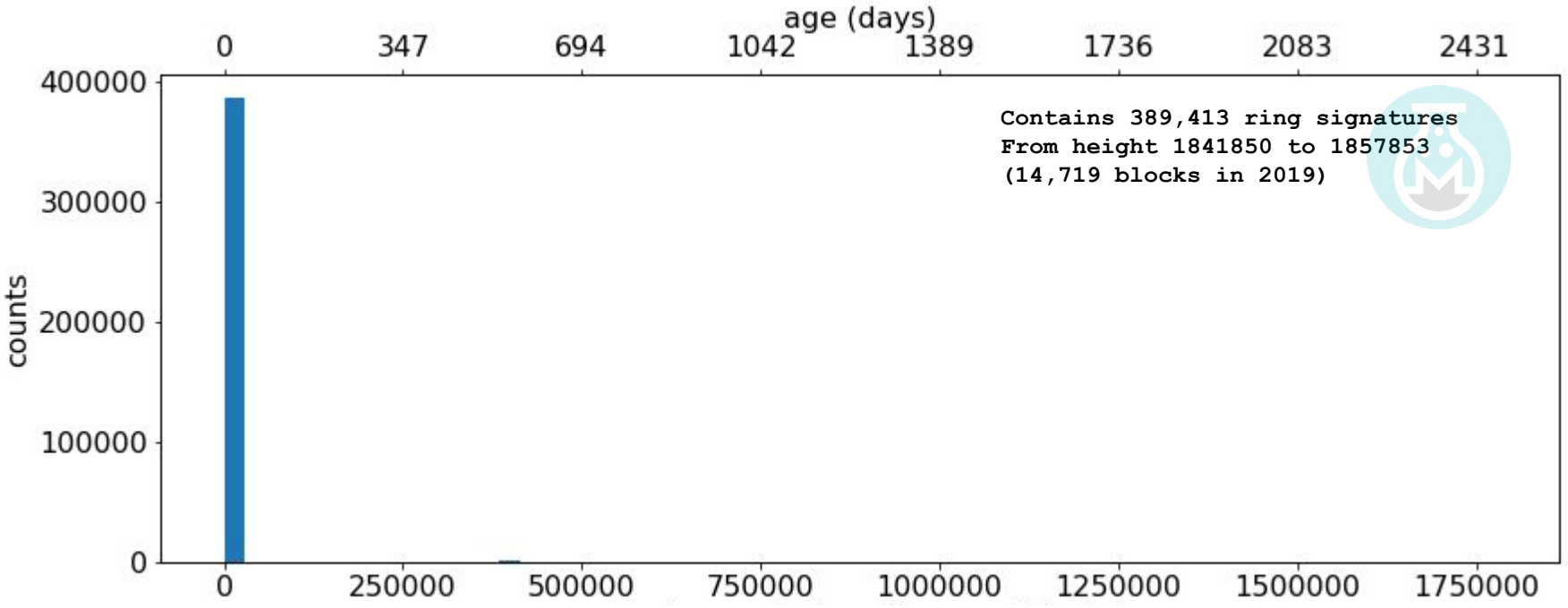
*Not to scale

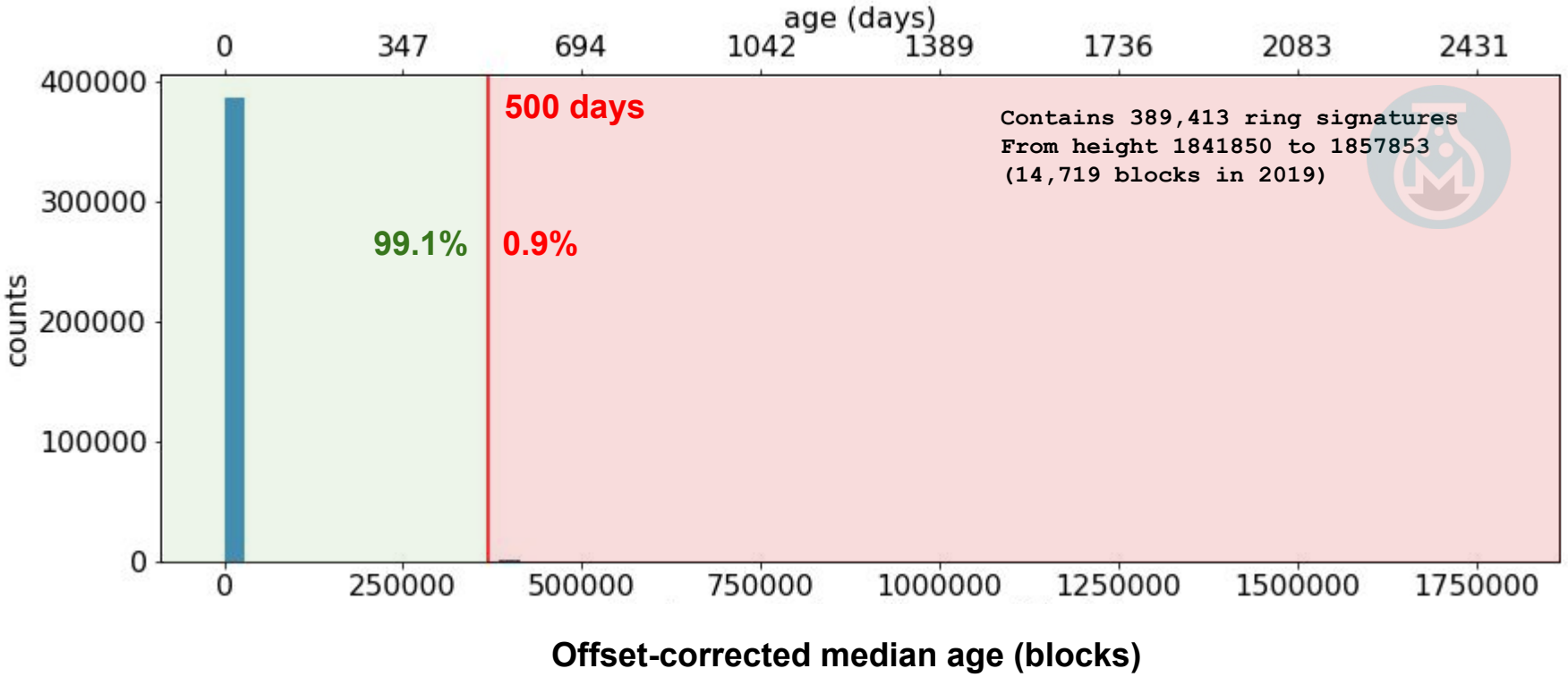
This is what outside observers can analyze:

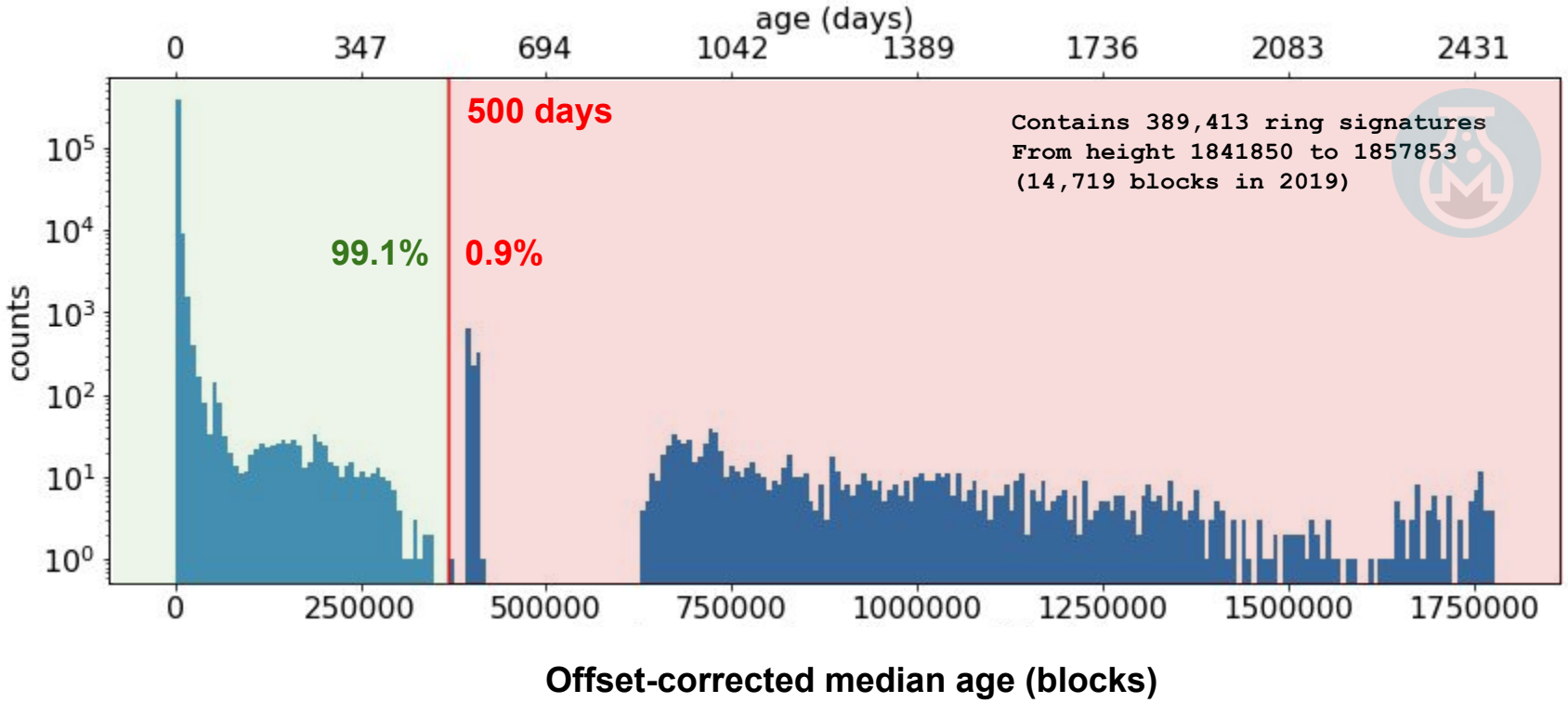


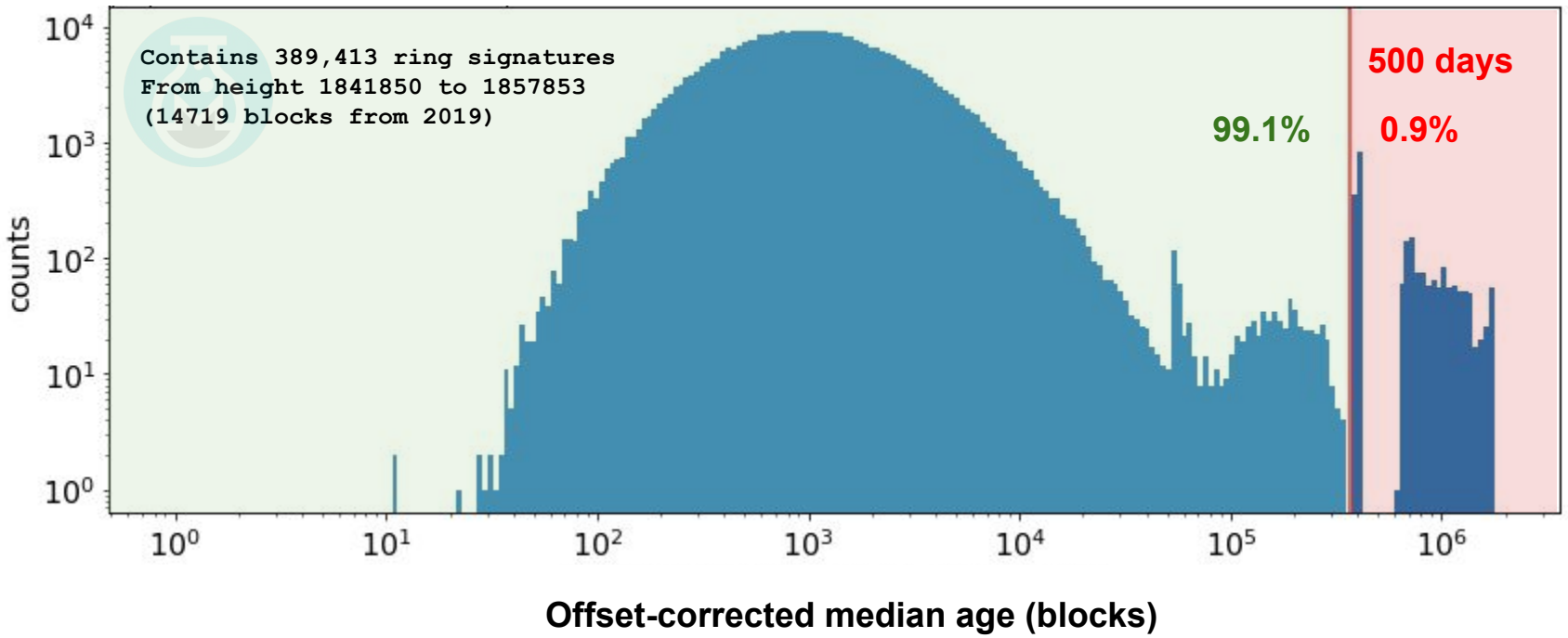
This is what outside observers can analyze:

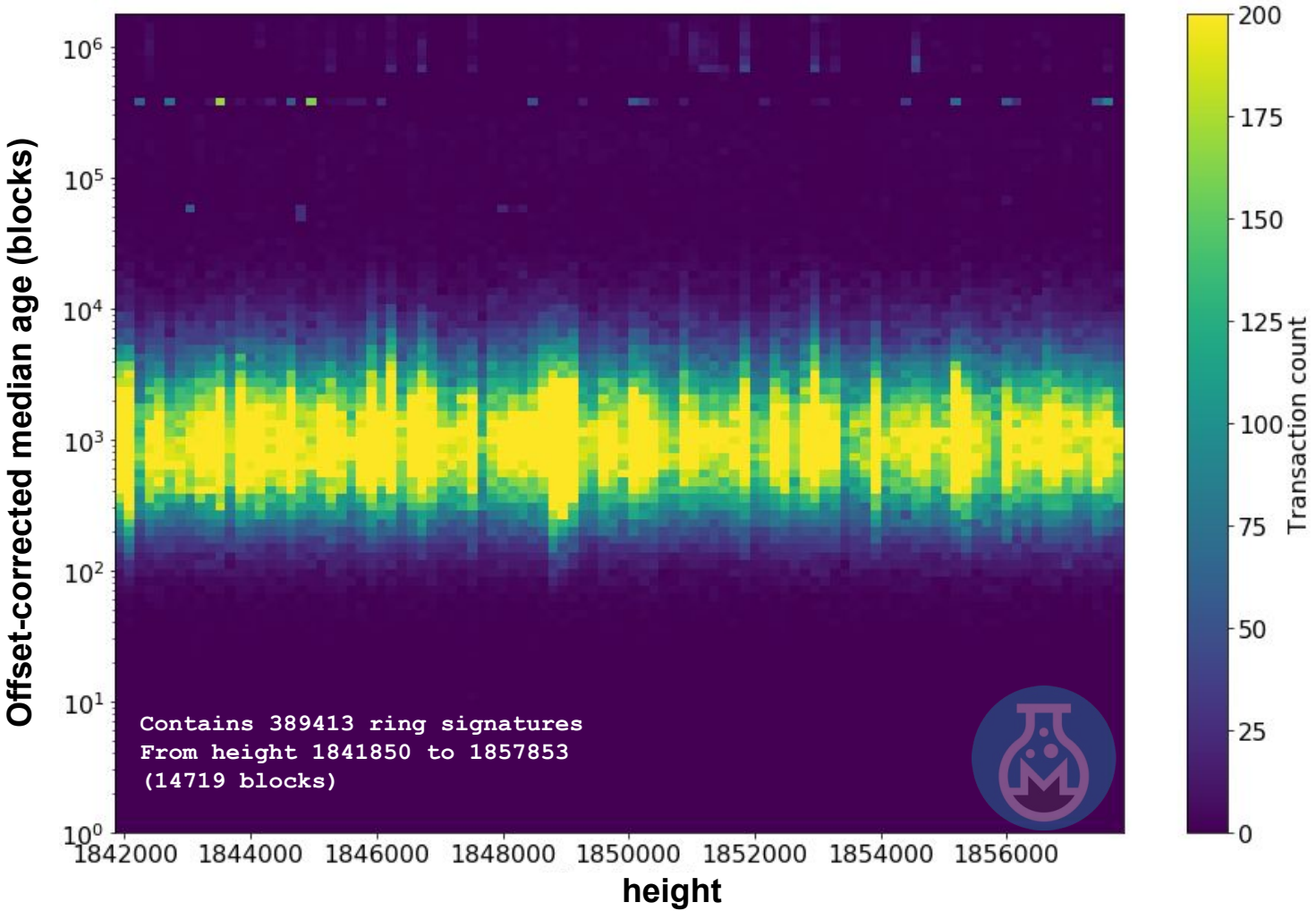


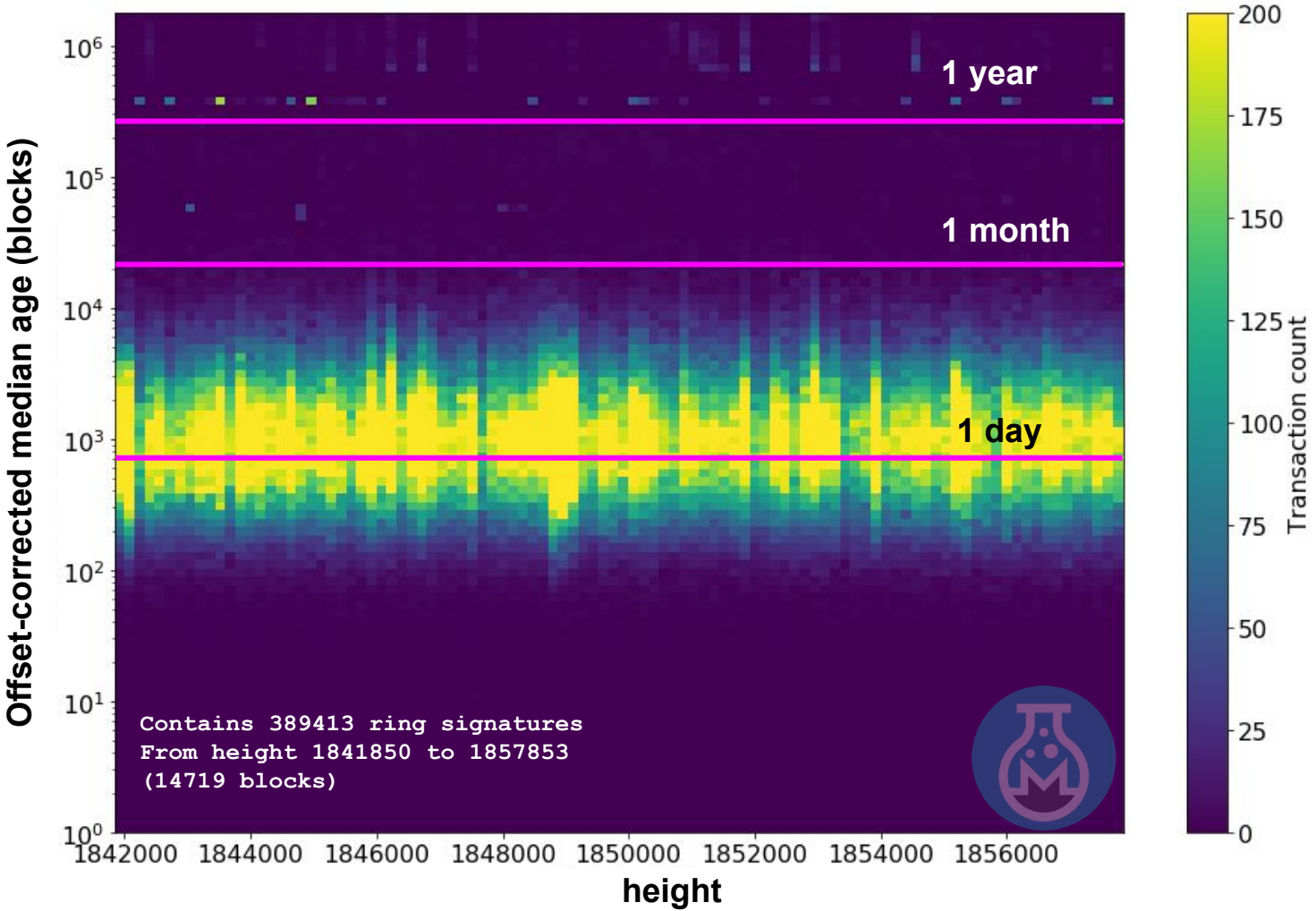

age (days)
0
347
694
1042
1389
1736
2083
2431
400000
300000
200000
100000
0
counts
Contains 389,413 ring signatures
From height 1841850 to 1857853
(14,719 blocks in 2019)
0
250000
500000
750000
1000000
1250000
1500000
1750000
Offset-corrected median age (blocks)

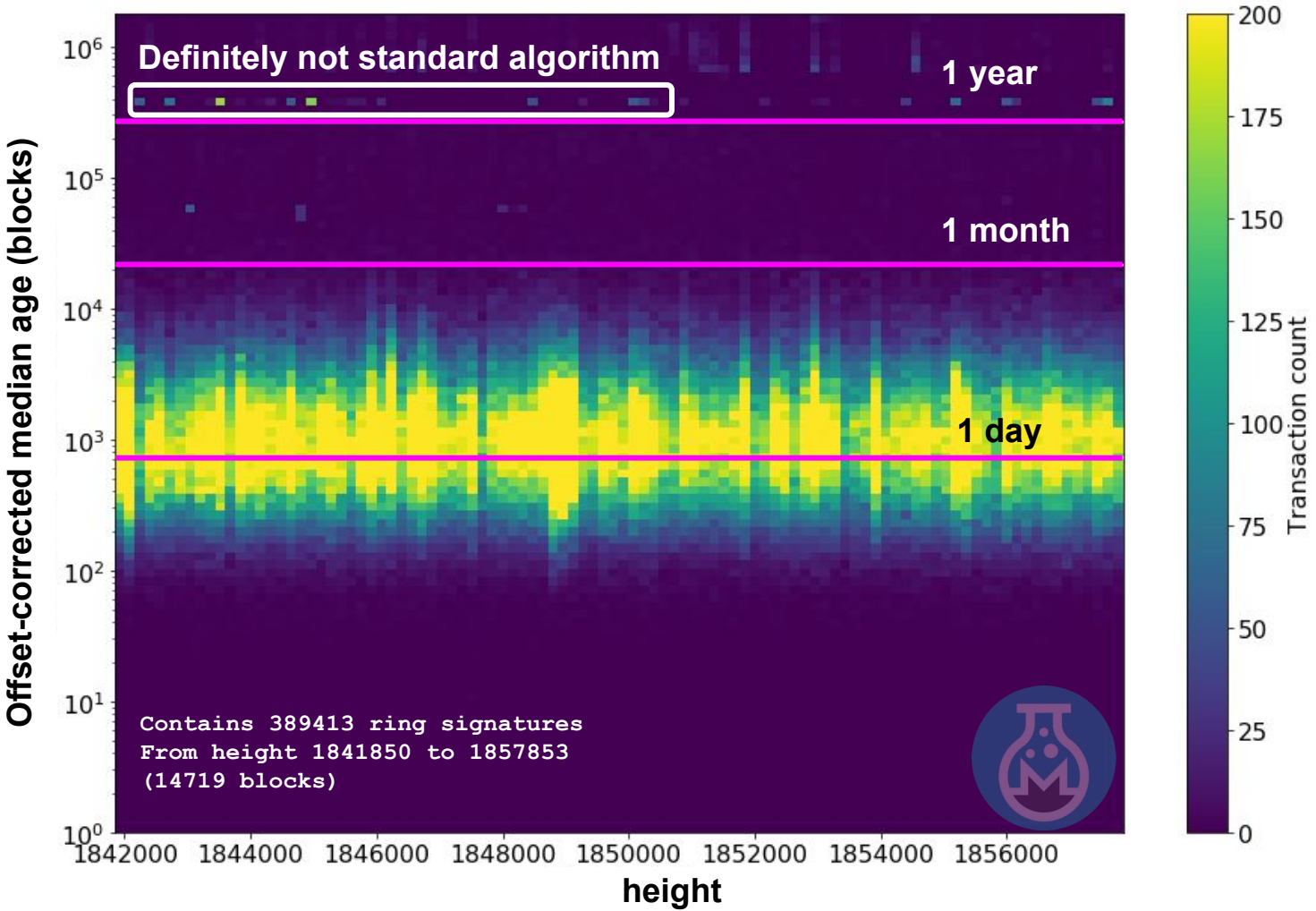

age (days)
0
347
694
1042
1389
1736
2083
2431
400000
300000
200000
100000
0
counts
500 days
99.1%
0.9%
Contains 389,413 ring signatures
From height 1841850 to 1857853
(14,719 blocks in 2019)
0
250000
500000
750000
1000000
1250000
1500000
1750000
Offset-corrected median age (blocks)


age (days)
0
347
694
1042
1389
1736
2083
2431
500 days
Contains 389,413 ring signatures
From height 1841850 to 1857853
(14,719 blocks in 2019)
99.1%
0.9%
counts
10^5
10^4
10^3
10^2
10^1
10^0
0
250000
500000
750000
1000000
1250000
1500000
1750000
Offset-corrected median age (blocks)


Contains 389,413 ring signatures
From height 1841850 to 1857853
(14719 blocks from 2019)
99.1%
500 days
0.9%
counts
10^0
10^1
10^2
10^3
10^4
10^5
10^6
Offset-corrected median age (blocks)


Offset-corrected median age (blocks)
10^6
10^5
10^4
10^3
10^2
10^1
10^0
1842000
1844000
1846000
1848000
1850000
1852000
1854000
1856000
height
Contains 389413 ring signatures
From height 1841850 to 1857853
(14719 blocks)
200
175
150
125
100
75
50
25
0
Transaction count


Offset-corrected median age (blocks)
10^6
10^5
10^4
10^3
10^2
10^1
10^0
1 year
1 month
1 day
Contains 389413 ring signatures
From height 1841850 to 1857853
(14719 blocks)
1842000
1844000
1846000
1848000
1850000
1852000
1854000
1856000
height
200
175
150
125
100
75
50
25
0
Transaction count


Definitely not standard algorithm
1 year
1 month
1 day
Contains 389413 ring signatures
From height 1841850 to 1857853
(14719 blocks)
Offset-corrected median age (blocks)
height
Transaction count
10^6
10^5
10^4
10^3
10^2
10^1
10^0
1842000
1844000
1846000
1848000
1850000
1852000
1854000
1856000
200
175
150
125
100
75
50
25
0

Act III Conclusions

- Vast majority (99.1%) of ring signatures use plausible distribution.
- Small anonymity puddles (0.9%) use distinctly irregular selection(s).

Act III Conclusions

- Vast majority (99.1%) of ring signatures use plausible distribution.
- Small anonymity puddles (0.9%) use distinctly irregular selection(s).
- Offset-corrected median is a robust method for identifying the worst offenders (= biggest privacy leaks).

Act III Conclusions

- Vast majority (99.1%) of ring signatures use plausible distribution.
- Small anonymity puddles (0.9%) use distinctly irregular selection(s).
- Offset-corrected median is a robust method for identifying the worst offenders (= biggest privacy leaks).
- Recommendation: Consensus protocol could reject transactions whose offset-corrected median age is more than some threshold.
- A very lenient threshold would be 360000 blocks (500 days), which would never reject properly-selected rings.

Act III Conclusions

- Vast majority (99.1%) of ring signatures use plausible distribution
- Small anonymity puddles (0.9%) use distinctly irregular selection(s).
- Offset-corrected median is a robust method for identifying the worst offenders (= biggest privacy leaks)
- Recommendation: Consensus protocol could reject transactions whose offset-corrected median age is more than some threshold.
- A very lenient threshold would be 360000 blocks (500 days), which would never reject properly-selected rings.
- (More strict standards are plausible, research pending)

Closing thoughts (high level)

- **Visualize your data, leverage your intuition!**

Closing thoughts (high level)

- **Visualize your data, leverage your intuition!**
- **Privacy protocol engineers:**
  - **Enforce necessary best practices in the consensus rules.**
  - **Don’t just hope 100% of devs match perfect reference implementation.**

Closing thoughts (high level)

- **Visualize your data, leverage your intuition!**
- **Privacy protocol engineers:**
  - **Enforce necessary best practices in the consensus rules.**
  - **Don’t just hope 100% of devs match perfect reference implementation.**
- **Privacy coin software developers:**
  - **Try to match the reference wallet.**
  - **Approximations or simplifications can leak a surprising amount of information.**

Closing thoughts (high level)

- Visualize your data, leverage your intuition!
- Privacy protocol engineers:
  - Enforce necessary best practices in the consensus rules.
  - Don’t just hope 100% of devs match perfect reference implementation.
- Privacy coin software developers:
  - Try to match the reference wallet.
  - Approximations or simplifications can leak a surprising amount of information.
- Users:
  - Use a community-vetted open-source wallet. See r/monero sidebar.
  - When in doubt, use the core software from www.getmonero.org
  - If you’re curious, look at your transaction on a block explorer.

INSIGHT

Decentralized Consensus
Fellows Program

InsightConsensus.com
(applications close soon)

Noncesense
Research Lab

INSIGHT

Decentralized Consensus
Fellows Program

InsightConsensus.com
(applications close soon)

Noncesense
Research Lab

Questions?

isthmus@getmonero.org

```
066E 5F6E 93A2 552E 8D81
486C 1518 F022 C296 0027
```

Slides and code will be available at:
k2019.noncesense.org