Bitcoin: A Peer-to-Peer Electronic Cash System

•••

Satoshi Nakamoto
2008

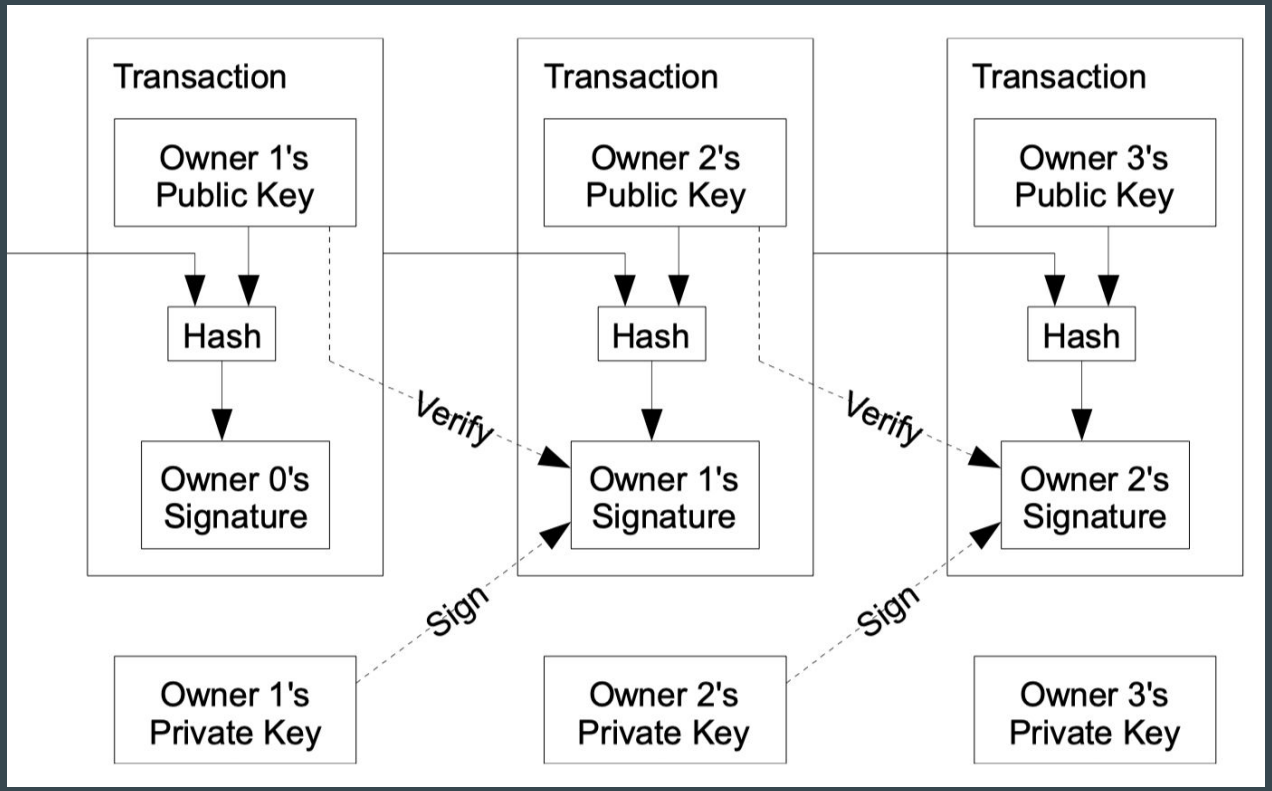
Presented By: Ayush Jain

P2P electronic cash system with no trusted third party

Problems ?

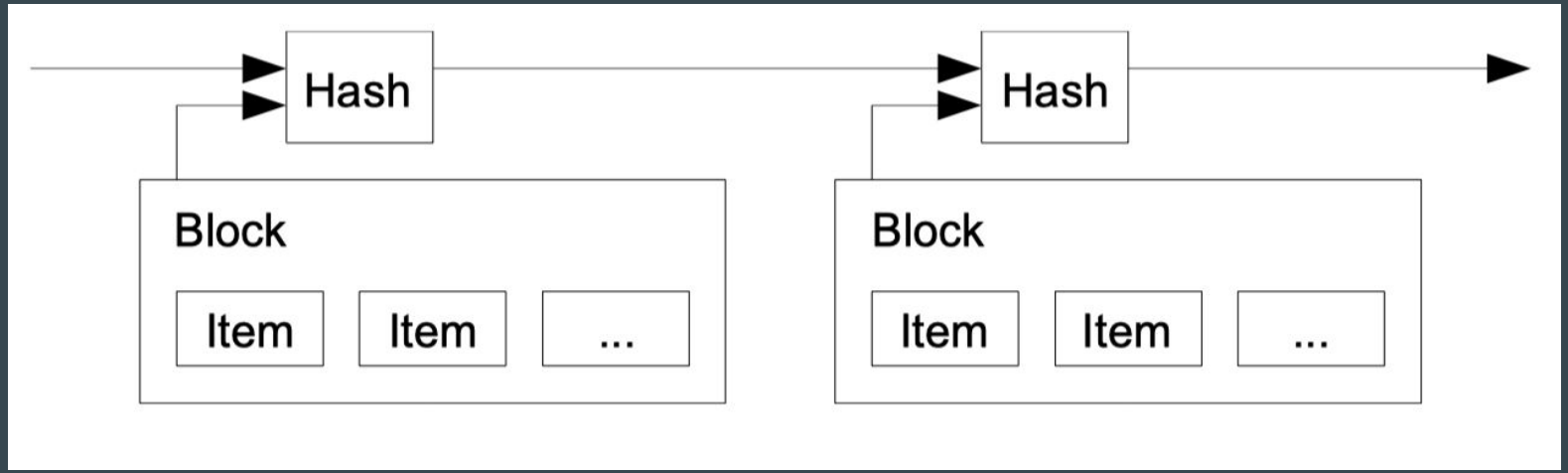
- ★ Track Ownership
- ★ Double Spending
  - ○ Race Attack
  - ○ Finney Attack
  - ○ 51% Attack

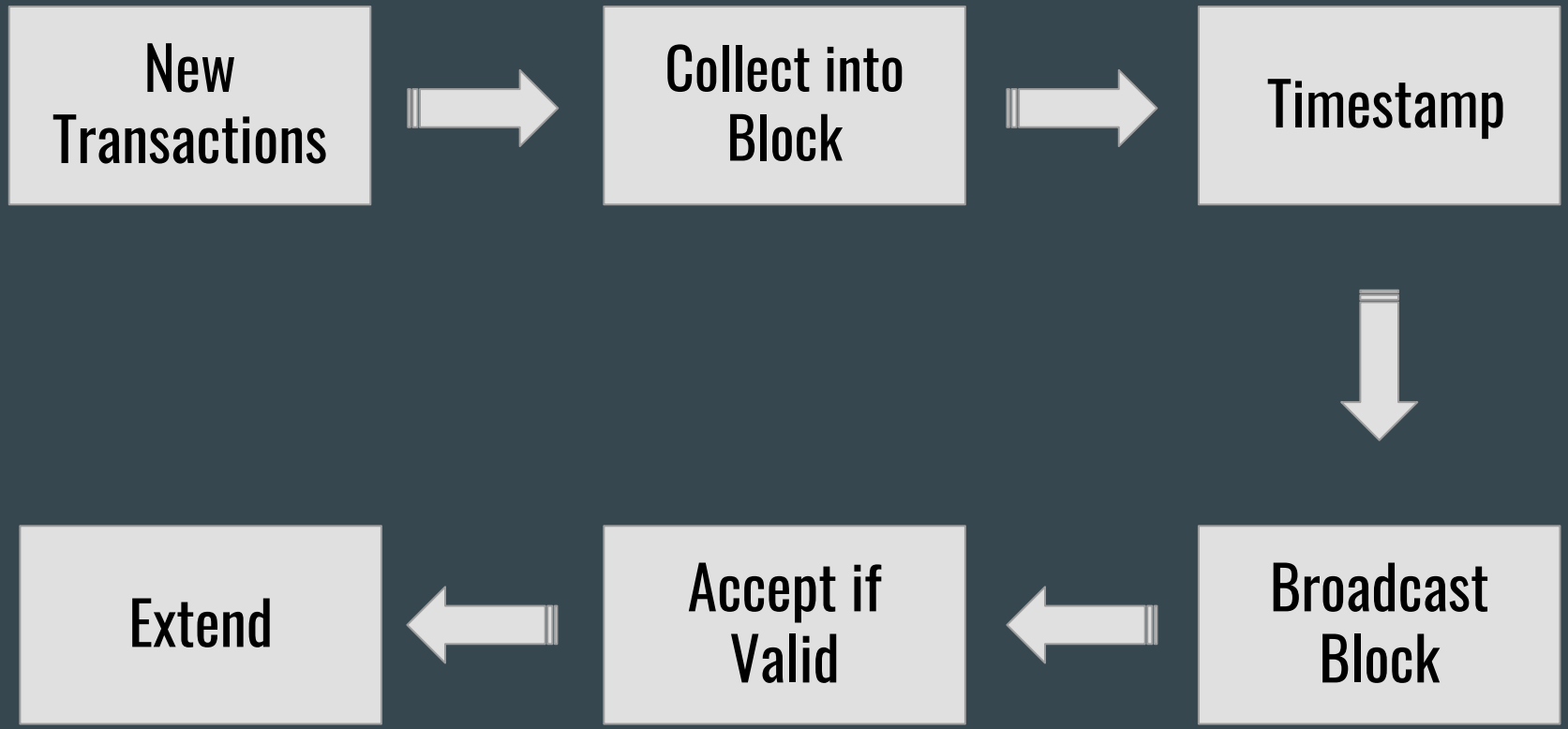
Coin Transaction



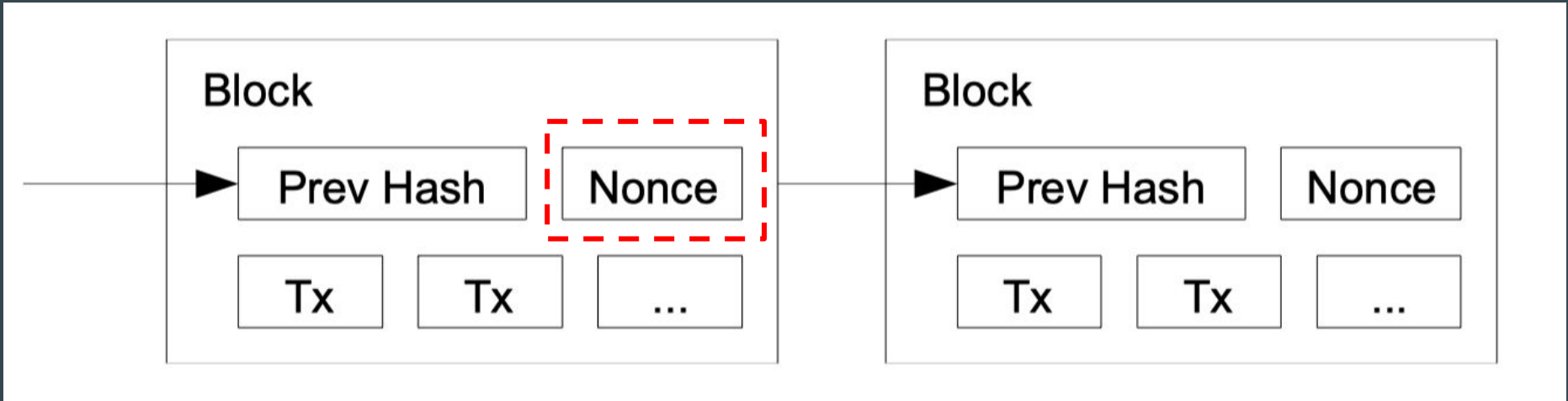
Block

- ★ A ledger of transaction data
- ★ Contains hash of the previous block
- ★ Finite size (~ 1 MB)




New Transactions
Collect into Block
Timestamp
Broadcast Block
Accept if Valid
Extend

Proof-of-Work



Properties

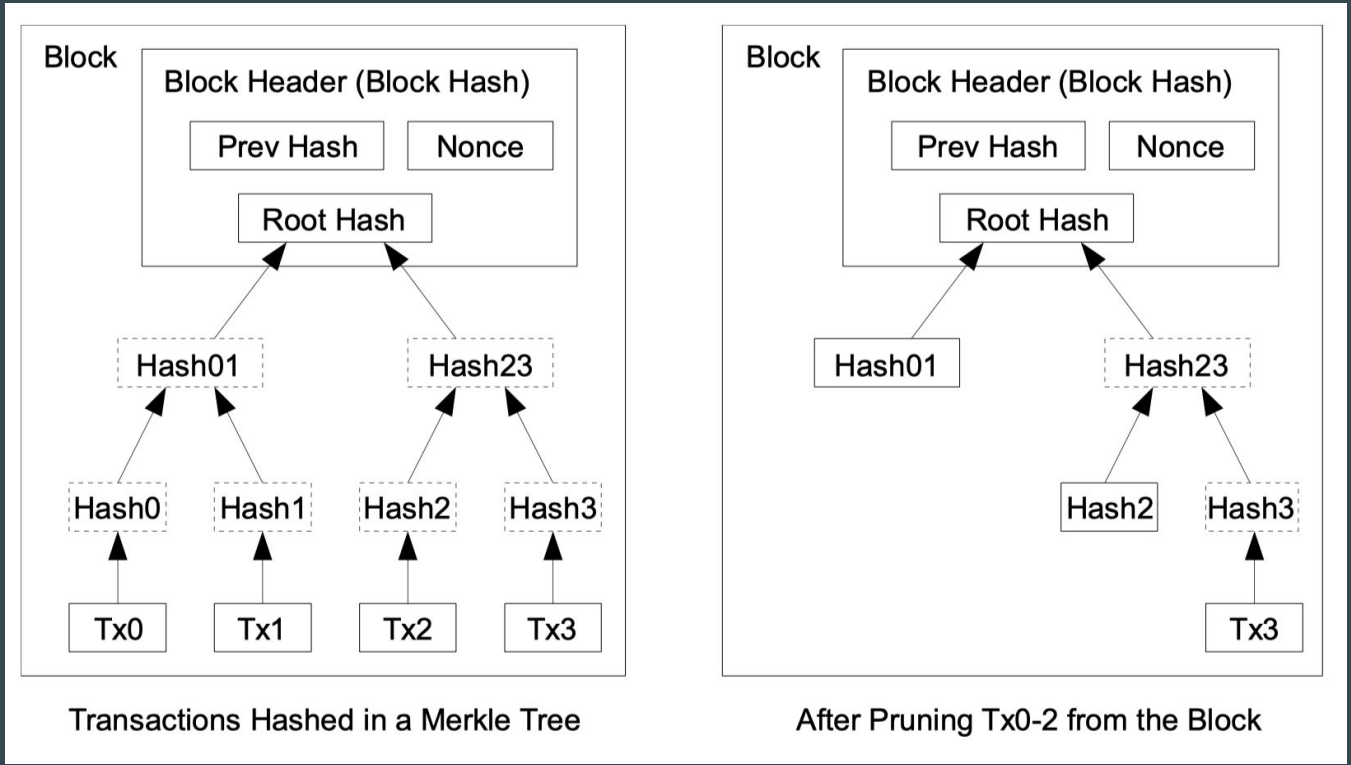
- ★ Target is currently 6.65 e+12
  - Lower value → exponentially greater difficulty
  - Readjusted every 2016 blocks (~ 2 weeks)
- ★ Impractical to rewrite history
- ★ No Guarantees

Why do the hard work ?

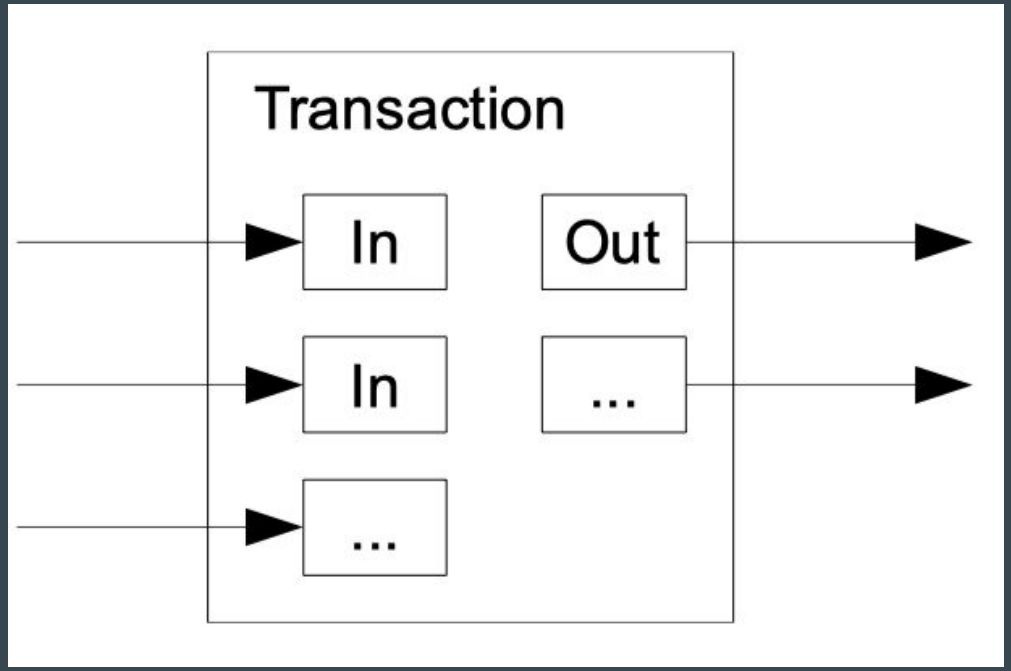
Incentives

- ★ Coinbase Transaction
  - 12.5 BTC (~ $46k) to the miner
  - 83% already mined.
  - Halves every 210,000 blocks
- ★ Transaction Fees
  - (Input Value - Output Value)
  - 10/30 minutes ~ 42 cents
  - 60 minutes ~ 26 cents

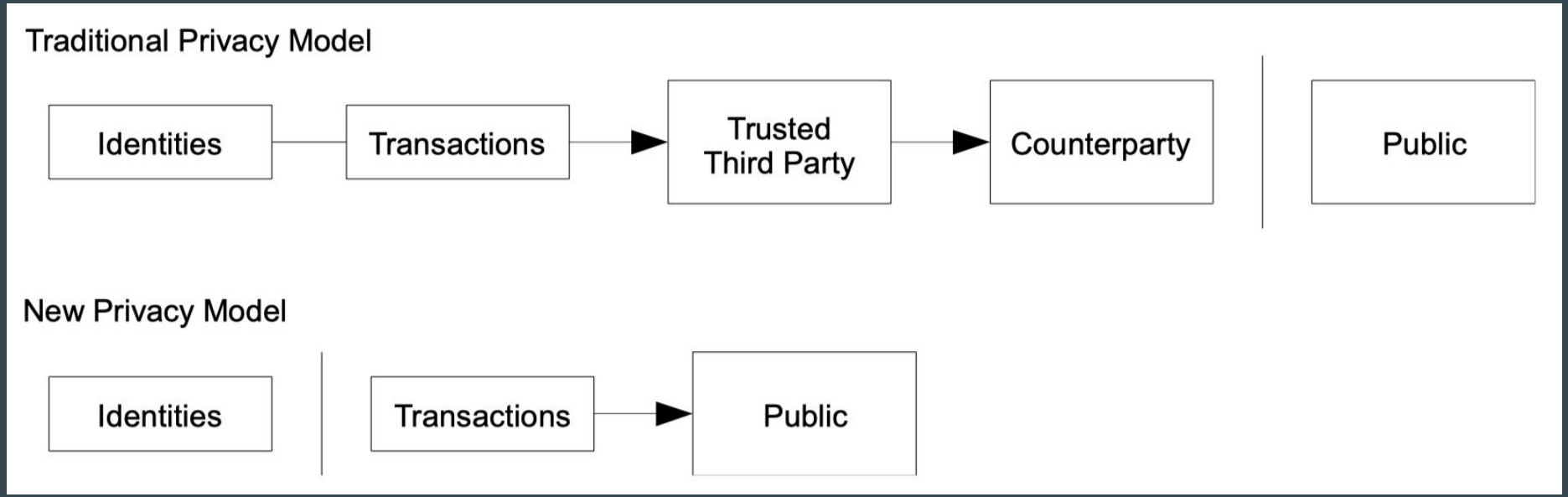
Saving Disk Space



Combining & Splitting Value



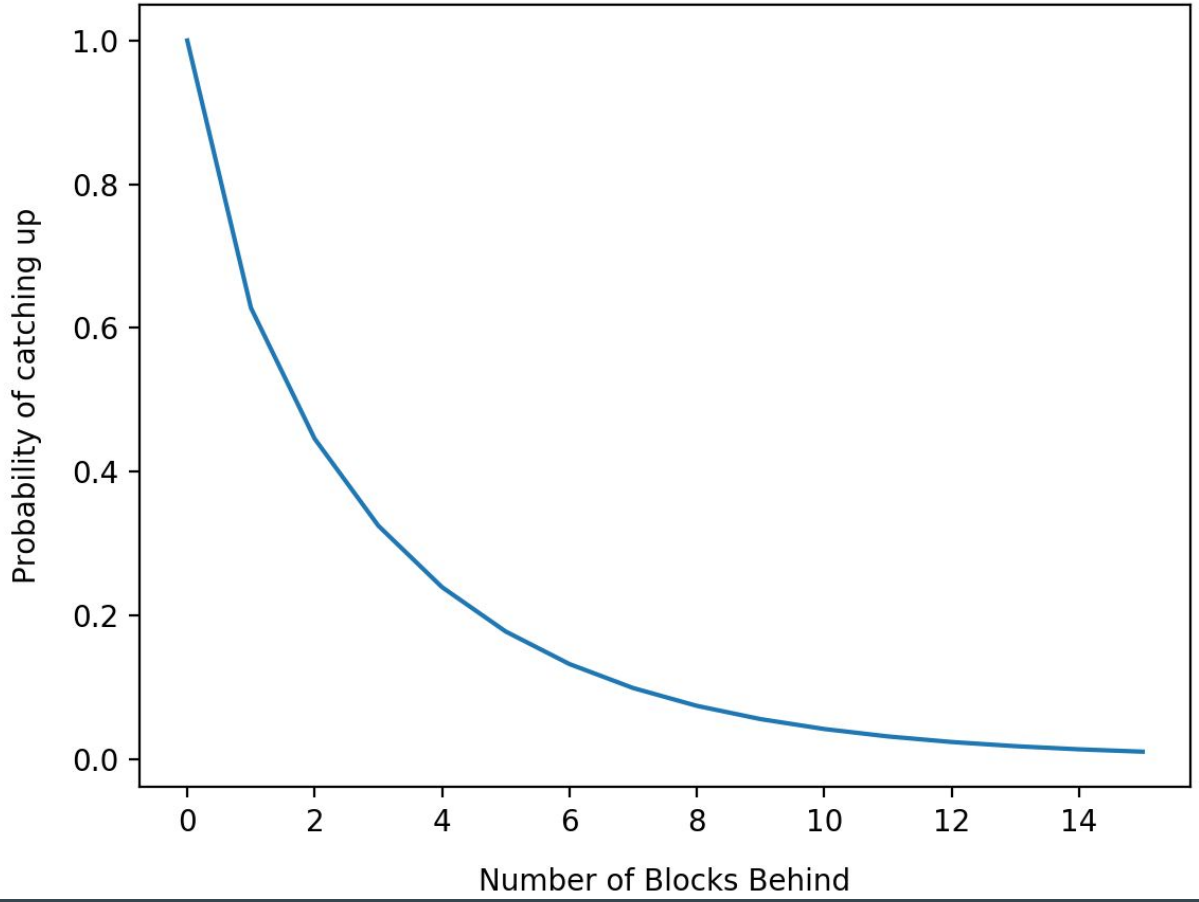
Privacy


Traditional Privacy Model
Identities
Transactions
Trusted Third Party
Counterparty
Public
New Privacy Model
Identities
Transactions
Public

Exponential Difficulty

p = probability an honest node finds the next block
q = probability the attacker finds the next block
z = number of blocks that have been linked after the transaction

$$1-\sum_{k=0}^{z}\frac{\lambda^{k}e^{-\lambda}}{k!}\left(1-(q/p)^{(z-k)}\right)$$


1.0
0.8
0.6
0.4
0.2
0.0
Probability of catching up
0
2
4
6
8
10
12
14
Number of Blocks Behind

Conclusion

- ★ Trust → ‘Cryptographic Proof’
- ★ Digital Signatures + PoW

Thank You