Bitcoin failure modes

and the role of the Lightning Network

Thaddeus Dryja, Joseph Poon

Scaling Bitcoin, Montreal 2015

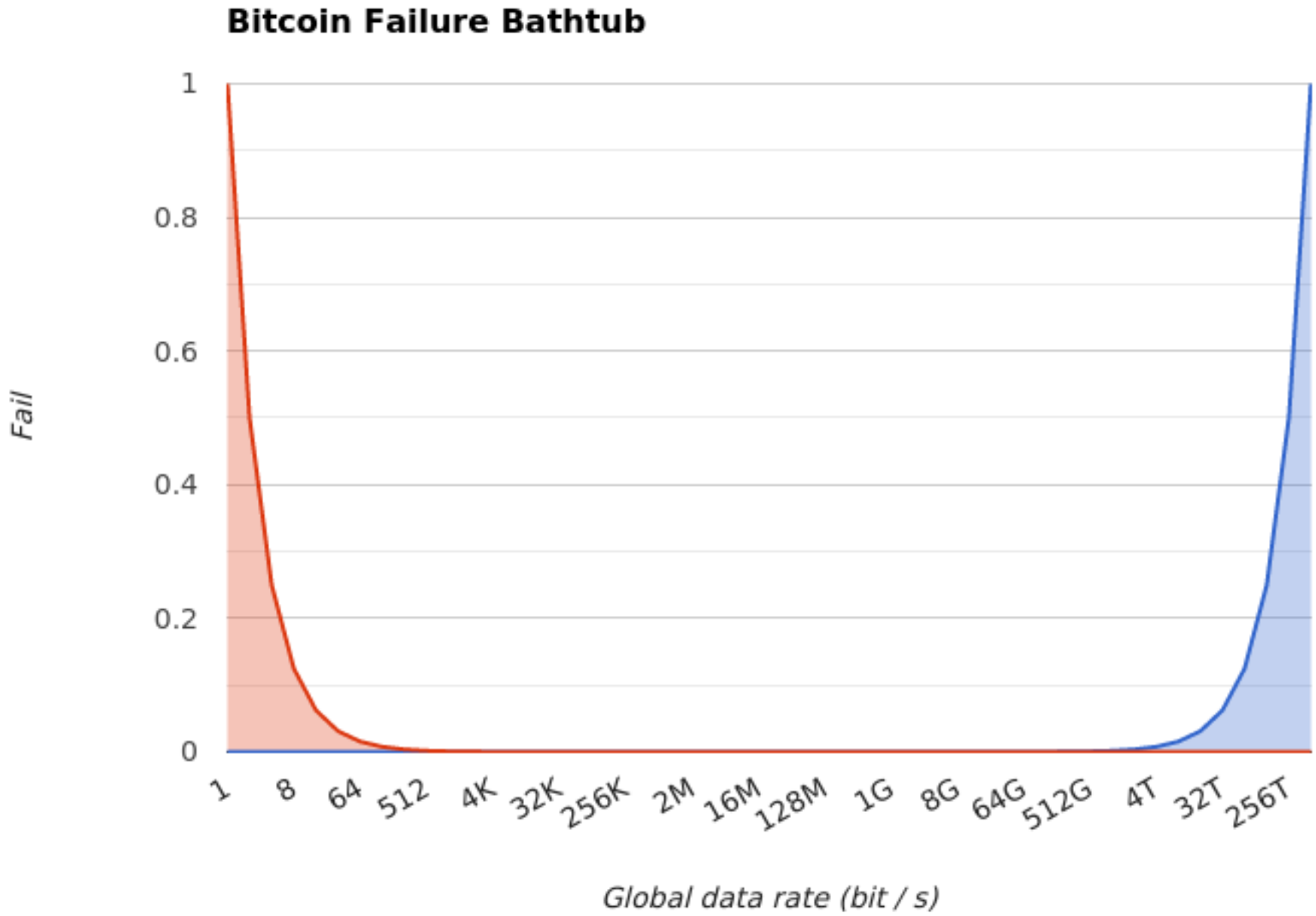
Bitcoin is working

- Transactions are propagated
- Blocks start with 00000000...
- Coins stay put, and then move when you send them
- That is so cool. I didn't think this would work.
- But it does! Great!

Bitcoin can fail

- But, but... anti-fragile!You mean... the final block?

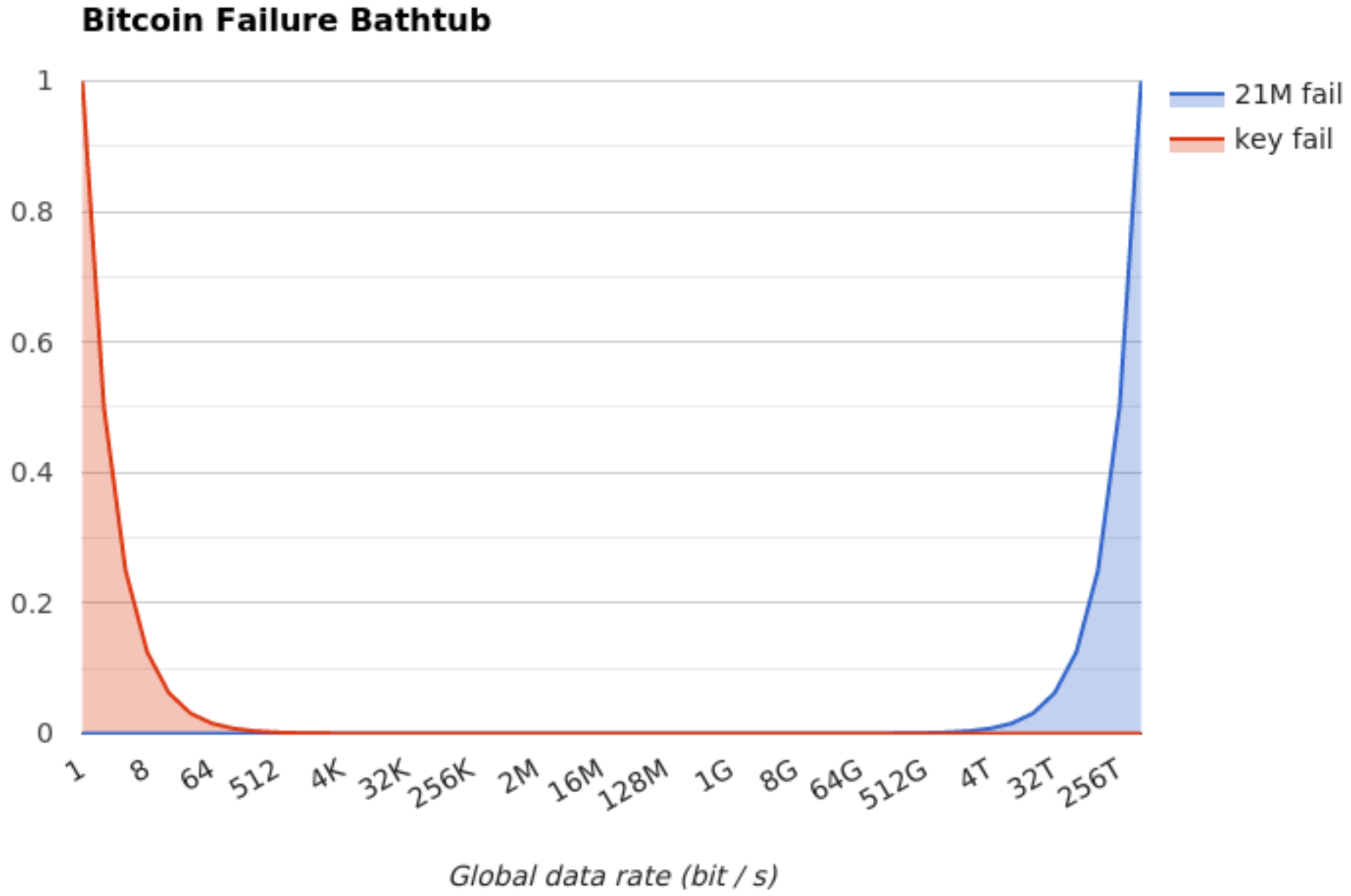
- There are fates worse than the end of blocks.


Bitcoin Failure Bathtub
1
0.8
0.6
0.4
0.2
0
Fail
1
8
64
512
4K
32K
256K
2M
16M
128M
1G
8G
64G
512G
4T
32T
256T
Global data rate (bit / s)

Block size bathtub

- Let's take extreme numbers.
- What would bitcoin be like with 1KB blocks? (~1 byte / sec)How about with 1PB blocks? (~1TB/sec)
- Both sides are bad. We can call both "failure".
- In both failure modes, assume every human on planet earth (~7Gh) would like to use bitcoin

(not a particularly pessimistic failure projection)


Bitcoin Failure Bathtub
1
0.8
0.6
0.4
0.2
0
21M fail
key fail
1
8
64
512
4K
32K
256K
2M
16M
128M
1G
8G
64G
512G
4T
32T
256T
Global data rate (bit / s)

Left side failure - key failure

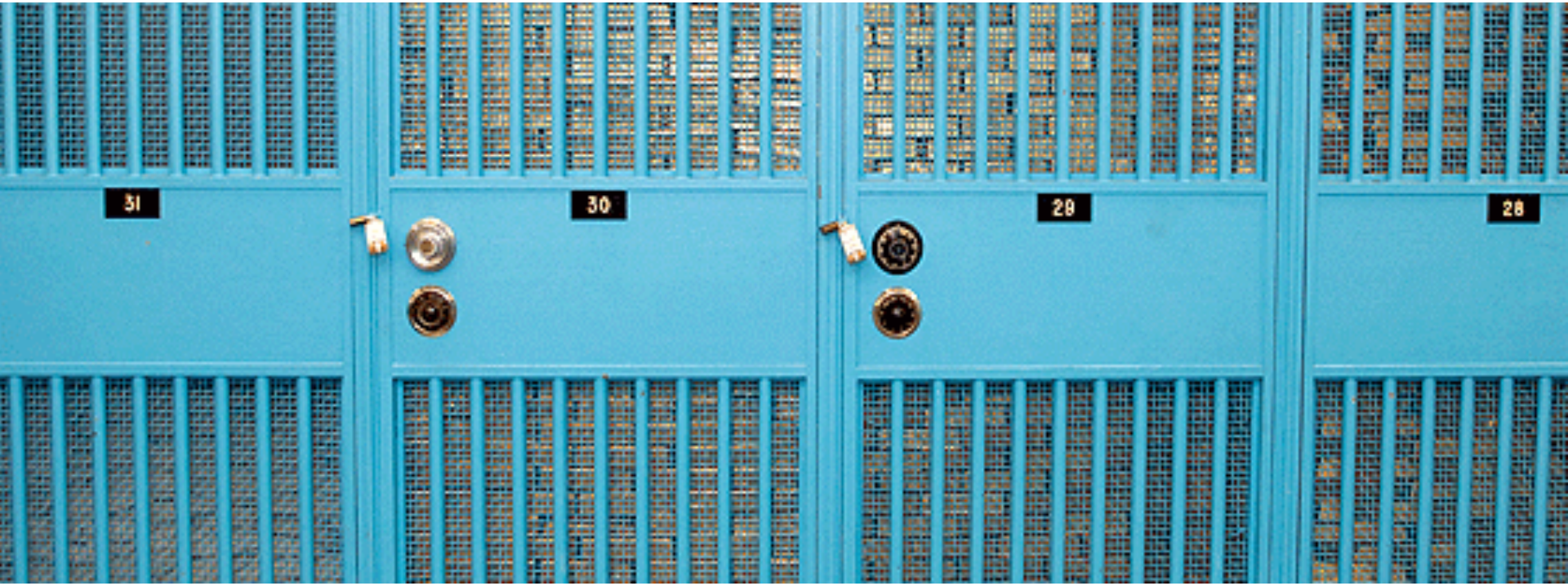
- 1tx / block means ~100 tx/day
- Block size increases by ~50MB / year
- Full blockchain can be verified on your phone. Great! But...
- ~10 large institutions have private keys to the UTXO set
- Coinbase, changetip, Bank of America, and BNY Mellon have keys.

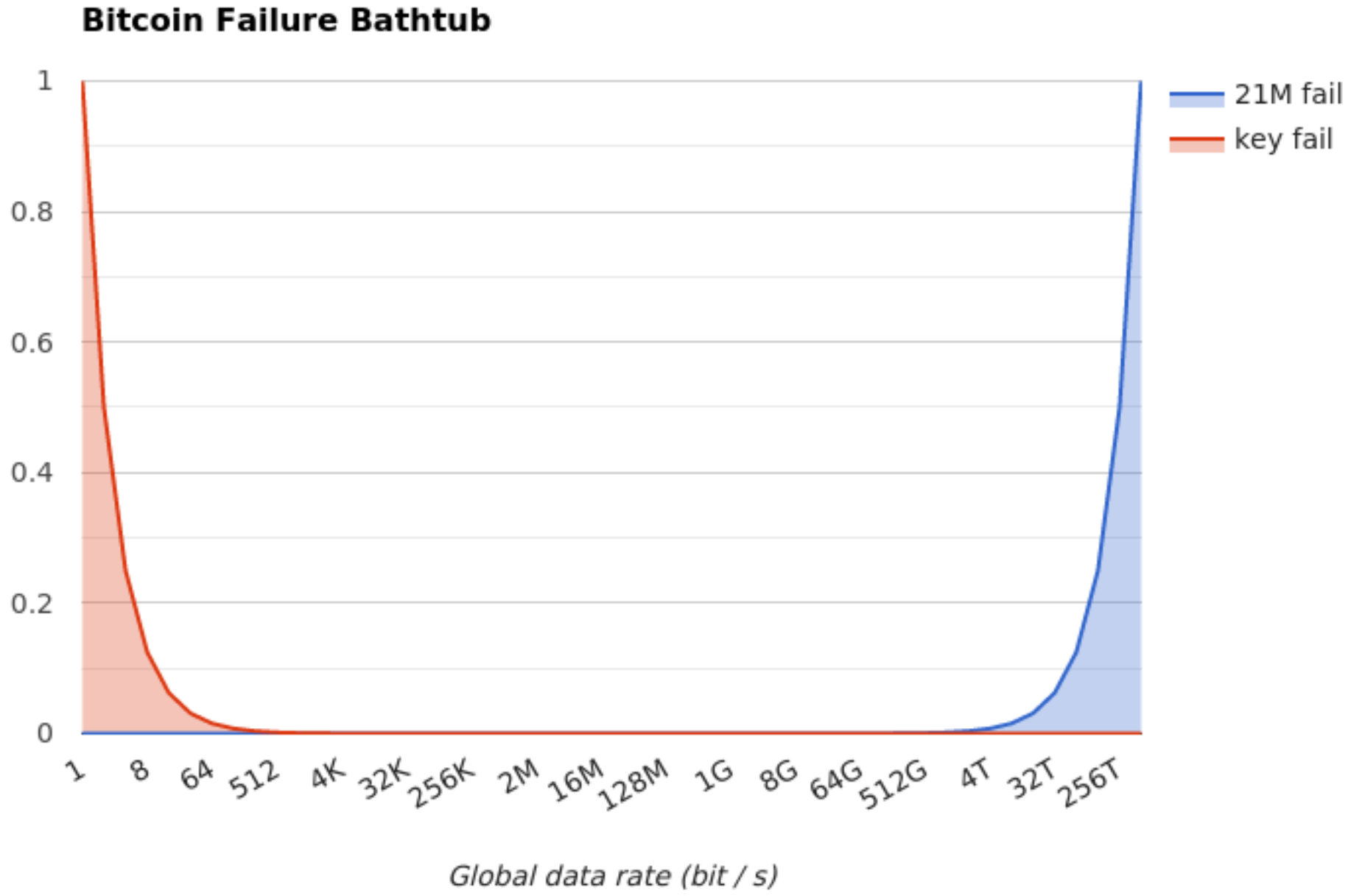
Left side failure - key failure

- How is this a failure?
- You don’t have the keys
  - You don’t have the coins. That was a central promise of bitcoin.
- You can’t be your own bank.
- You can, however, verify all balances that your bank holds for you.

Left side failure - Good delivery model

Left side failure - Good delivery model




Bitcoin Failure Bathtub
1
0.8
0.6
0.4
0.2
0
21M fail
key fail
1
8
64
512
4K
32K
256K
2M
16M
128M
1G
8G
64G
512G
4T
32T
256T
Global data rate (bit / s)

Right side failure - 21M failure

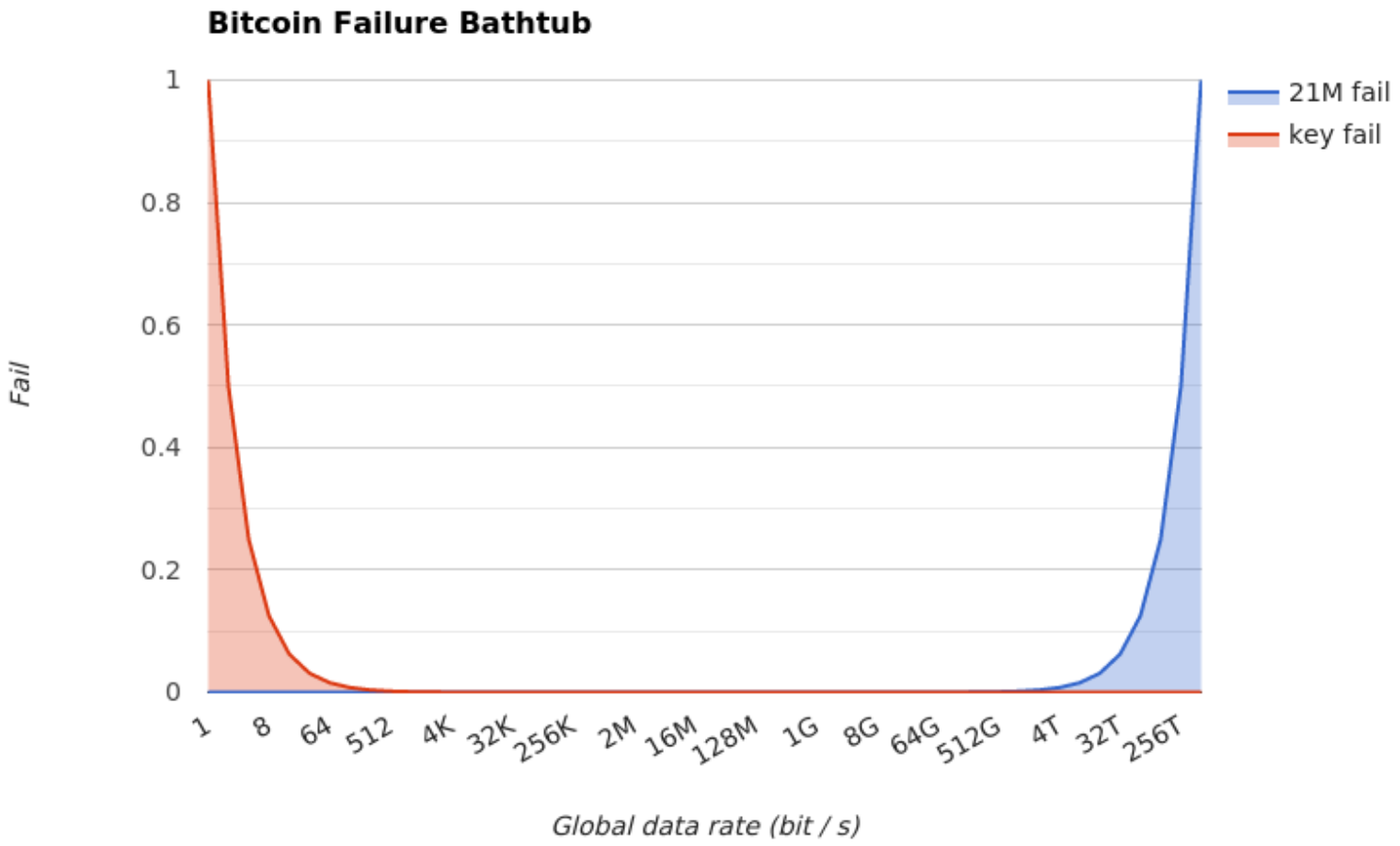
- All 7Gh can use bitcoin many times a day for any transaction. Everyone has their own private keys on their phone.
- ~50 EB/year expansion of blockchain.
- SPV proofs are still quite compact, phones can store the header set (~4MB/yr)

Right side failure - 21M failure

- ~10 large institutions can store and verify the blockchain.
- While you have lots of keys, Amazon, Visa, Google, Bank of America, and UnionPay are the ones who have the blockchain.
- You can verify when you receive coins. But you can't verify everyone else's. Are you sure there are still 21M coins? No double spends anywhere?

Right side failure - Bureau of Engraving and Printing model

Expanding the bathtub



(bathtub not to scale)

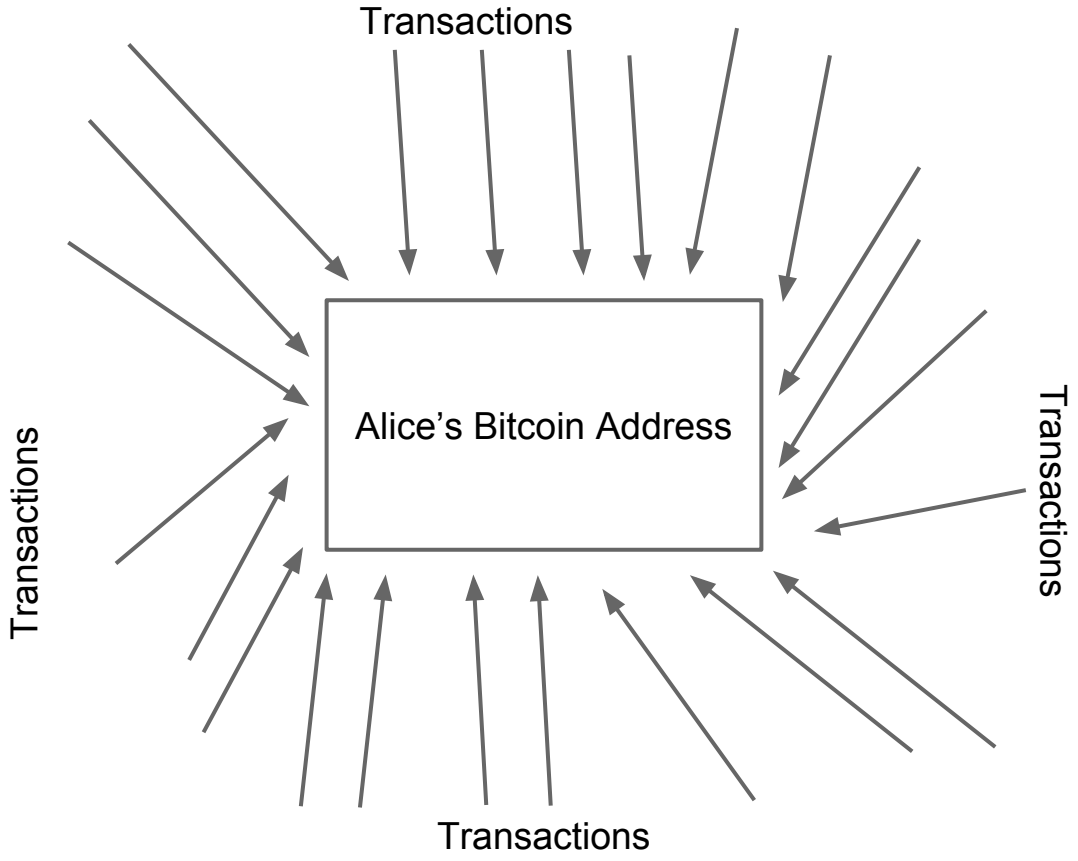
Expanding the bathtub

- How can we expand usability without hurting verifiability
- Methods to have more user to user transactions with lower global verification cost
- Linked nodes of payment channels is one way to expand the bathtub to the left (reduce need to increase global throughput)

Bitcoin Payment Networks

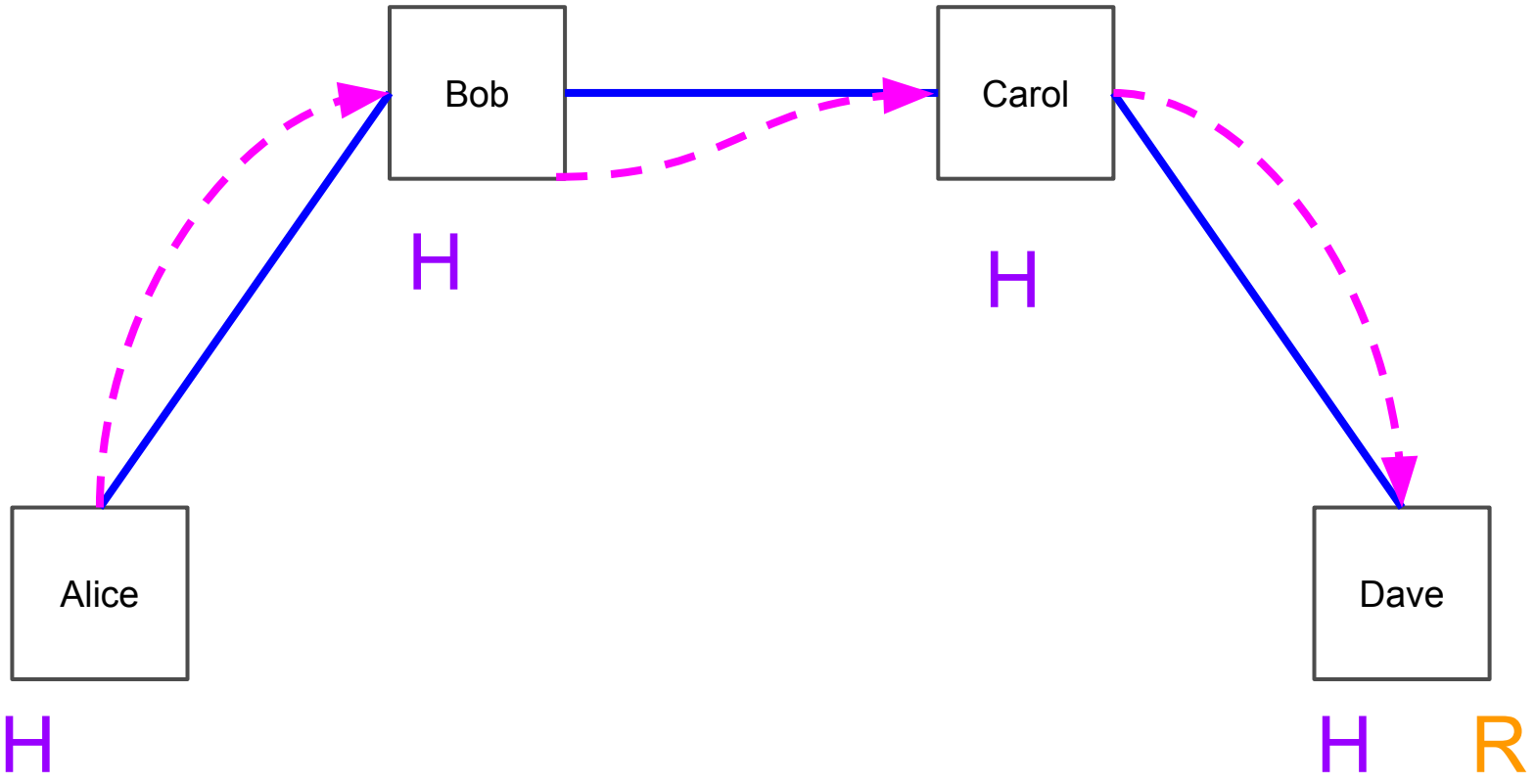
- E.g. Lightning Network
- Widens the bathtub sweet spot
- Problems which it helps with:
  - Net settle many transactions
  - Micropayments which are below the minimum fee ($0.01 micropayment with $0.03 bitcoin blockchain transaction fees)
  - Fee Market?
  - UTXO set bloat...

Micropayment UTXO Set Bloat



No problem, right? What happens when you want to spend these transactions? You need to include each one as an input. What if each input is a couple cents? These transactions would be insane!

Lightning Network

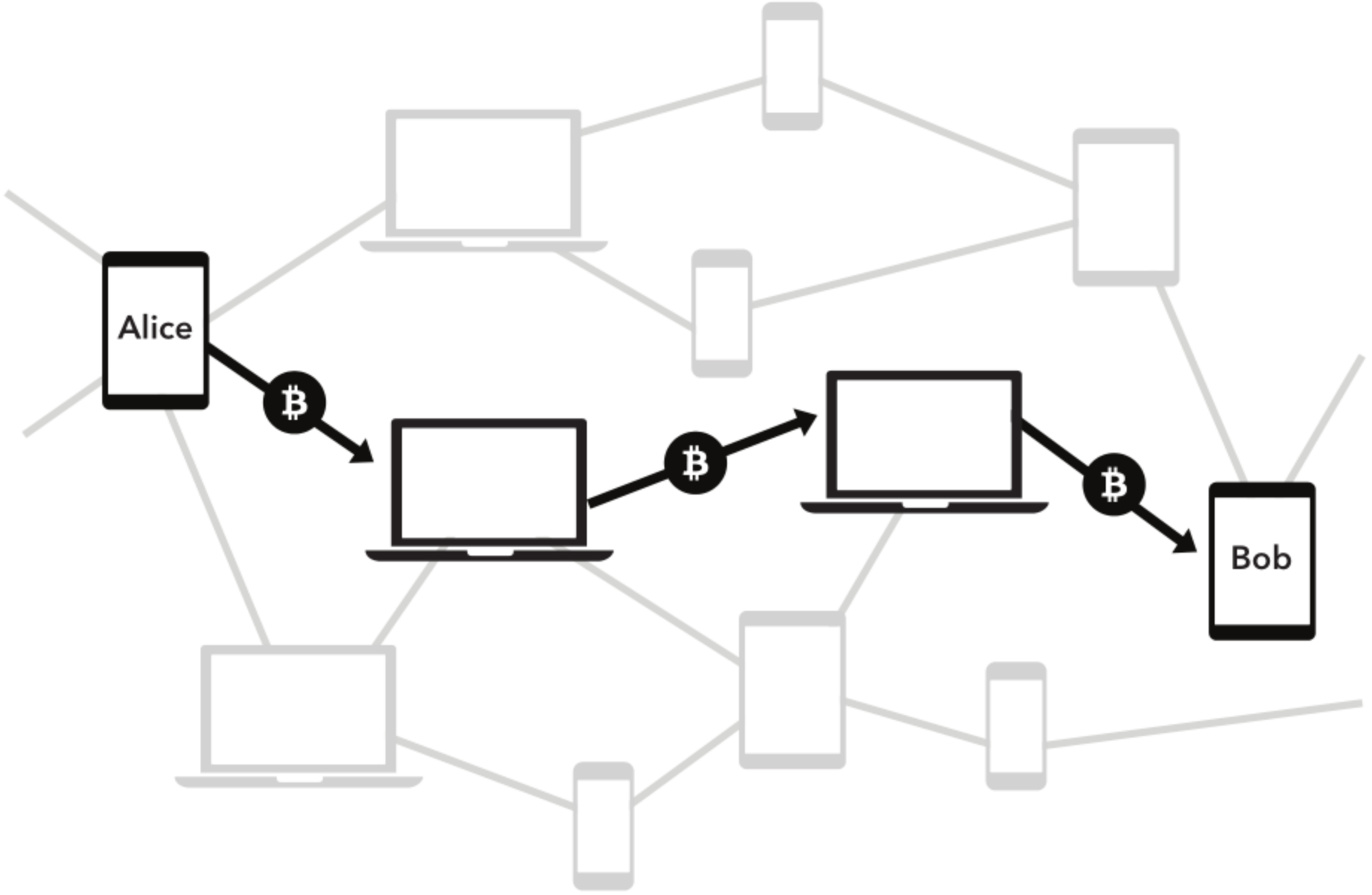


Decentralized Bitcoin Payment Networks

- While these are actual bitcoin transactions with consensus enforced on the blockchain, payment path selection is local
- Why do we need it to be decentralized?
  - Bitcoin’s values
  - We need to ensure there’s no custodial ownership
    - Open participation
    - Anyone can run a node
    - Extremely low fees

Decentralized Bitcoin Payment Networks

- Trusting a 3rd party custodian with your balance (or payments in transit) will be giving them a lot of economic rent
- **Routing** behavior is a local protocol among participants (local consensus)
  - Therefore it's necessary to ensure and enforce routing and node selection is fairly decentralized.
- Make sure all wallets are also channel nodes, to ensure decentralization


Alice
Bob