Ten Years of Bitcoin
Evaluating its performance as a monetary system

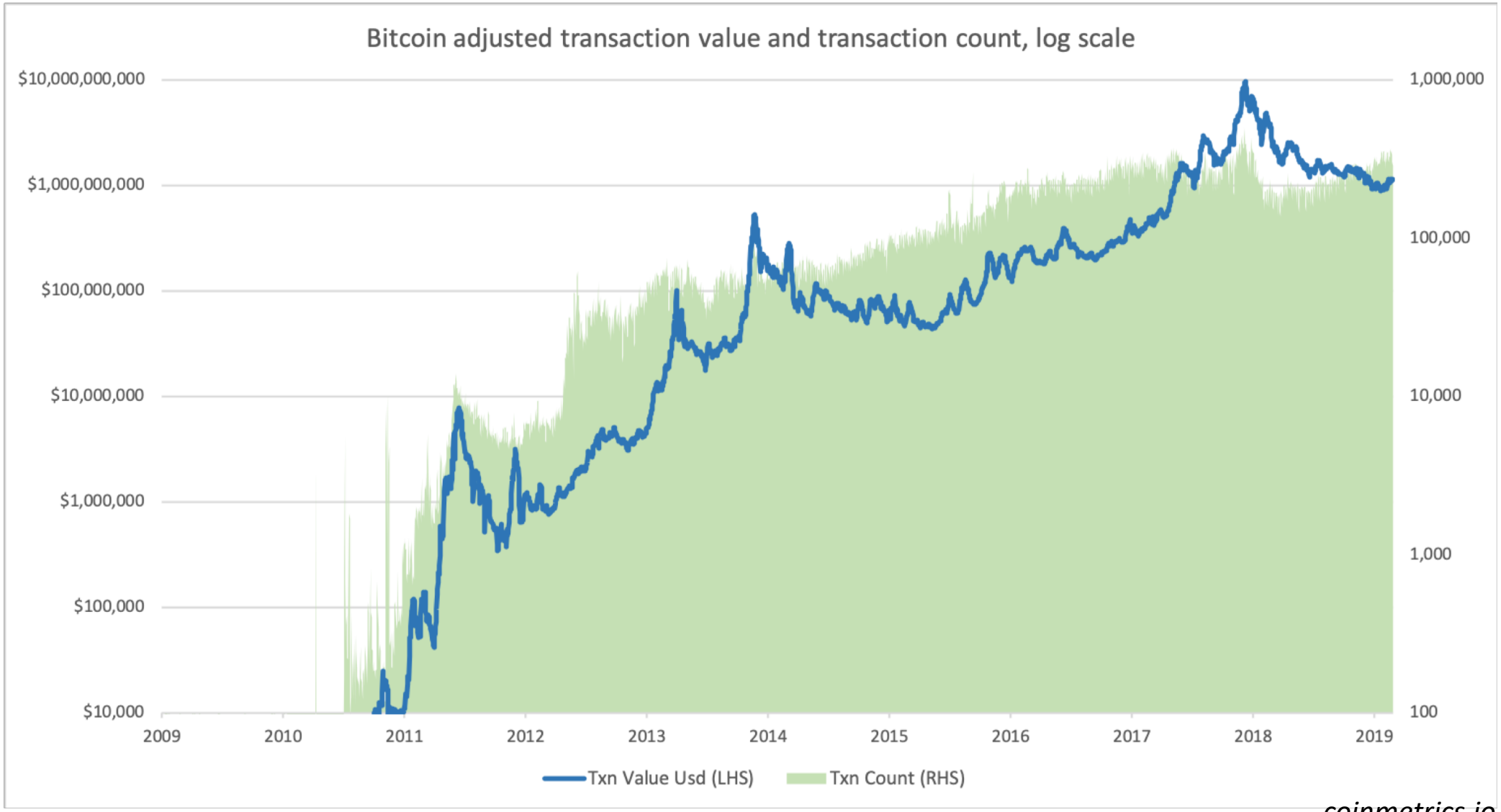
MIT Bitcoin Club

The next 1010 years

CASTLE ISLAND
VENTURES

Nic Carter

A successful first decade



coinmetrics.io

Bitcoin’s looming fee market

- On everyone’s mind: what will transaction fees have to reach to support our current security spend?
- Wait… why are we indexing fees to our current security spend? It’s just a function of price…
- Is our current security spend too high? Too low?
- Wait… what is Bitcoin’s long-term security model in the first place?

Bitcoin's security model

Satoshi Nakamoto:

"If a majority of CPU proof-of-worker is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains."

Satoshi only considers a 51% attack in his paper. But other attacks and motives exist!

- Nation state attacks
- Short seller attack + sabotage

How should these be modeled, and how do they affect the security budget?

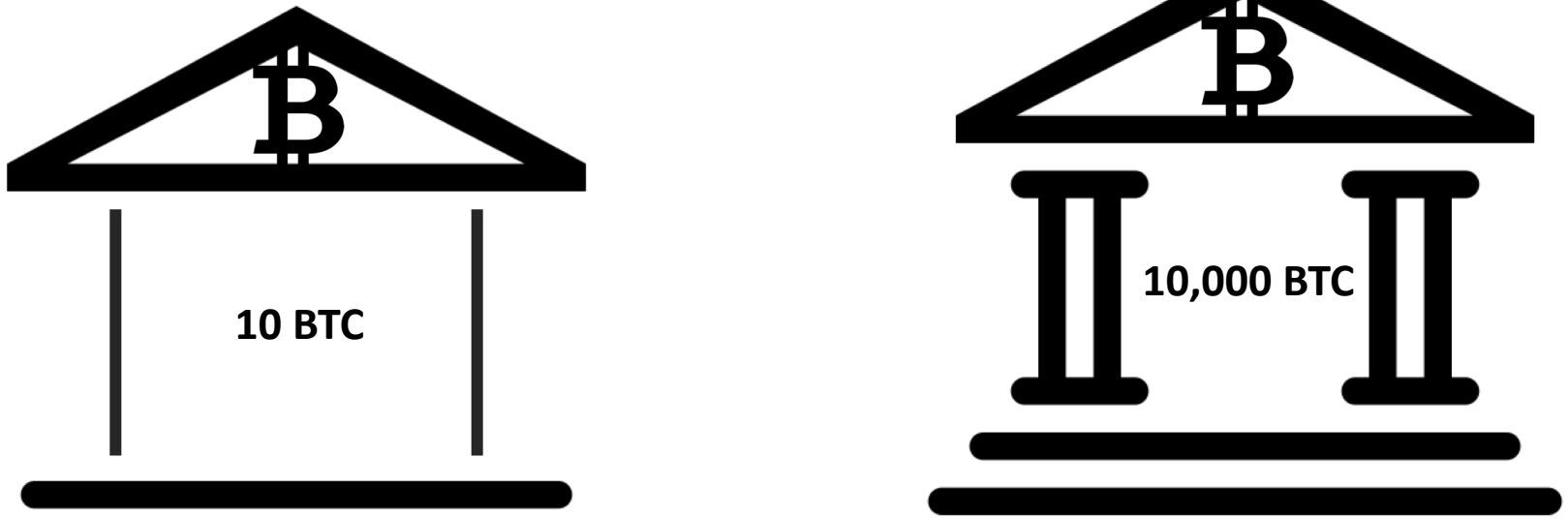
Three broad approaches to security

- **Threshold:** At a given level of security spend, Bitcoin is assumed secure
  - At a given threshold, no entity can marshal sufficient resources (electricity, ASICs, mining farms) to overpower the honest majority
- **Stock:** Security spend should be indexed to the value of Bitcoin itself
  - The returns from attacking bitcoin are a function of the value of bitcoin, so security spend should grow with the aggregate value
- **Flow** (*Budish*[1]): fees must be large relative to transactional volume
  - Rewards from 51% attacks (which are a function of txn value) must be offset by high fees to honest miners
  - Fees will therefore be prohibitively high

[1.] Budish, Eric. The economic limits of bitcoin and the blockchain. No. w24717. National Bureau of Economic Research, 2018.

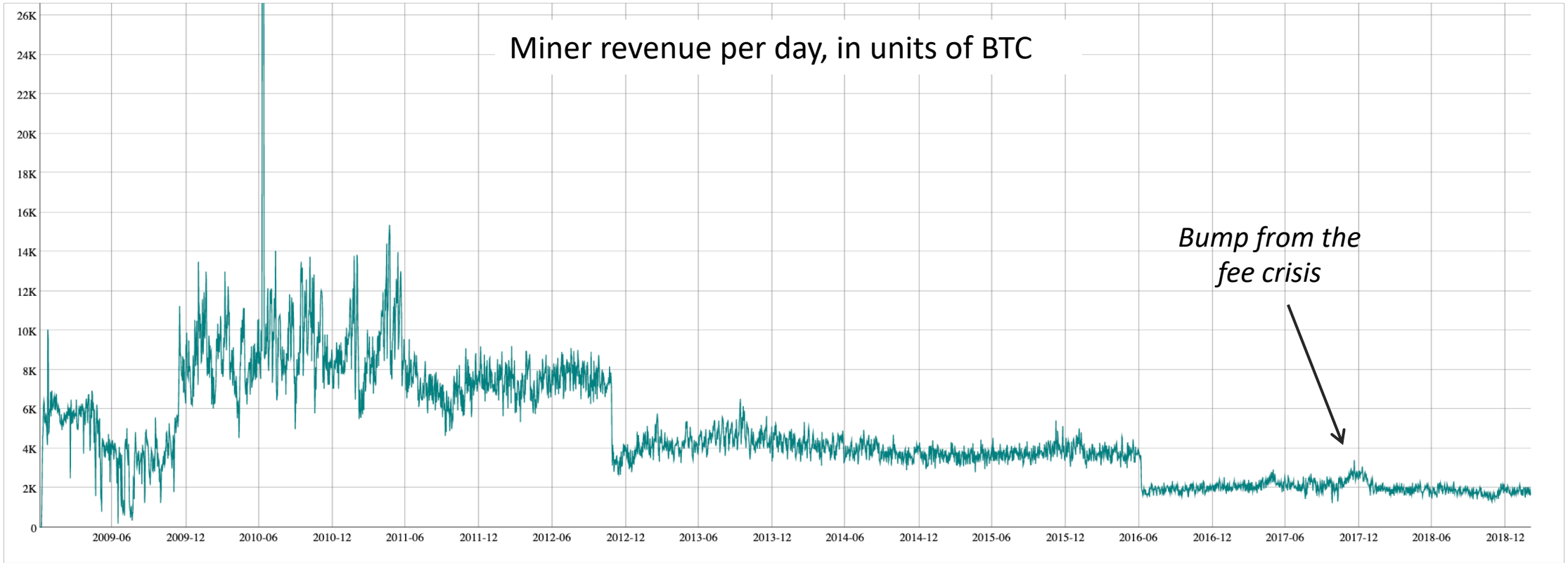
The threshold model

The stock model



- The security expenditure should vary with value of the asset being stored
- Since Bitcoin can be sold short in liquid markets, the value of a successful attack varies with the market value of Bitcoin itself
- So Bitcoin should index security expenditure to market capitalization
  - But this isn't how Bitcoin works!

Bitcoin's relative security expenditure keeps dropping... by design



coinmetrics.io

Fees will constitute Bitcoin's security budget

Satoshi Nakamoto:

*"Once a predetermined number of coins have entered circulation, the **incentive can transition entirely to transaction fees** and be completely inflation free."*

"In a few decades when the reward gets too small, the transaction fee will become the main compensation for nodes."

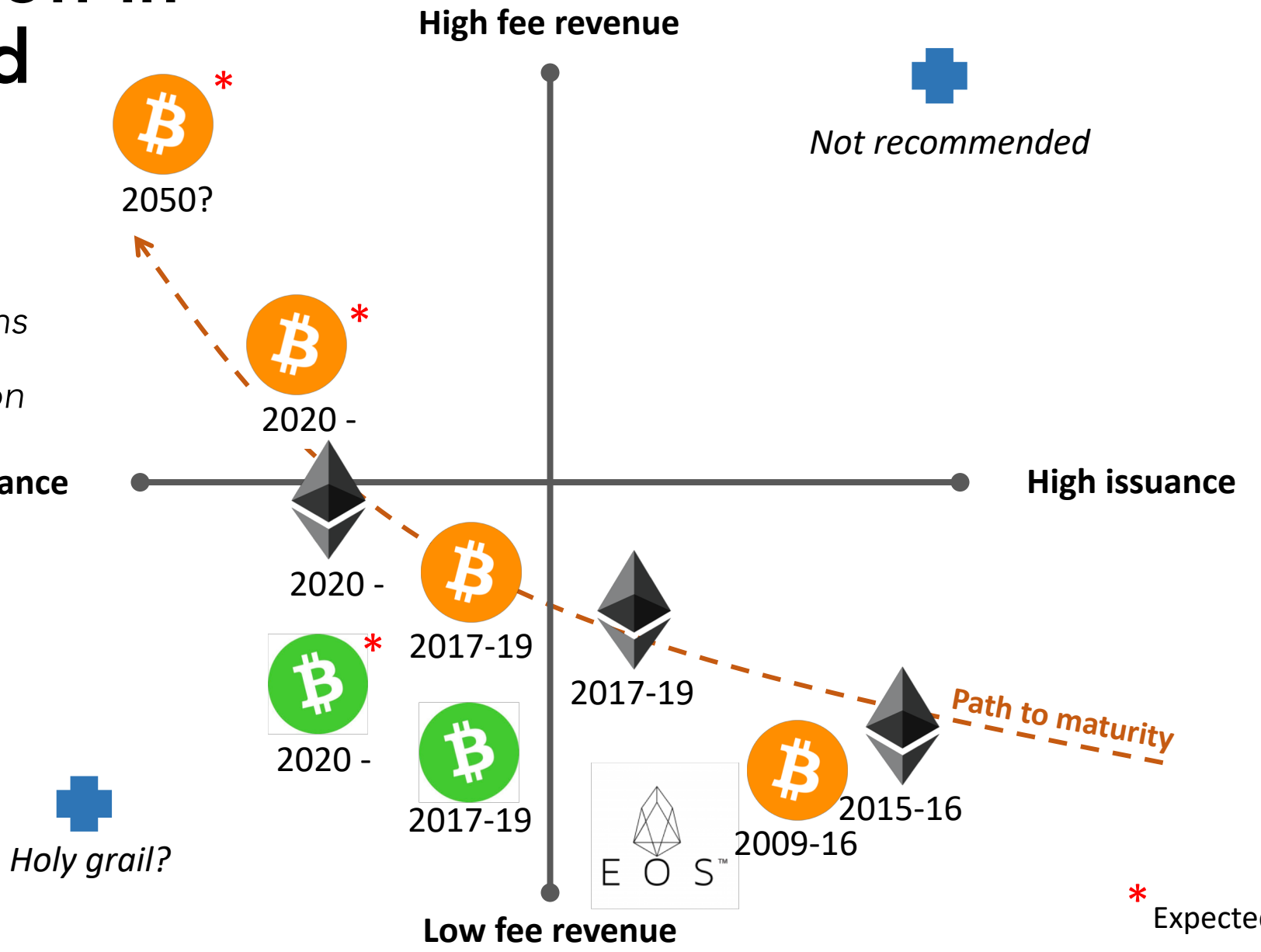
Greg Maxwell:

"Fee pressure is an intentional part of the system design and to the best of the current understanding essential for the system's long term survival."

Fees ensure scarcity in the long term!

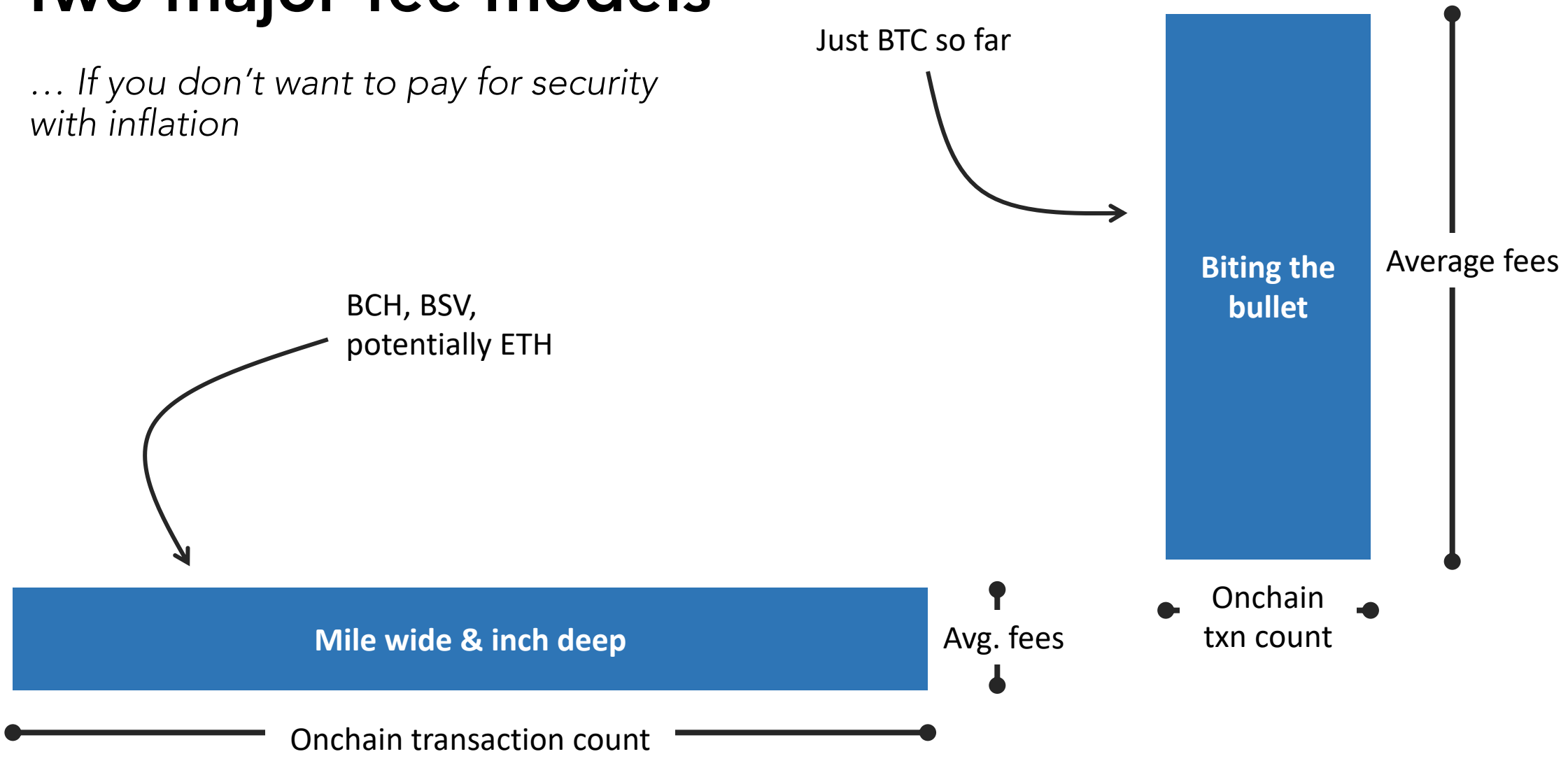
The big tradeoff in security spend

- *You can subsidize miners/validators with fees or issuance*
- *Long term, major chains intend to reduce issuance and will rely on fees*



Two major fee models

… If you don't want to pay for security with inflation



Can Bitcoin charge a premium for block space?

Yes

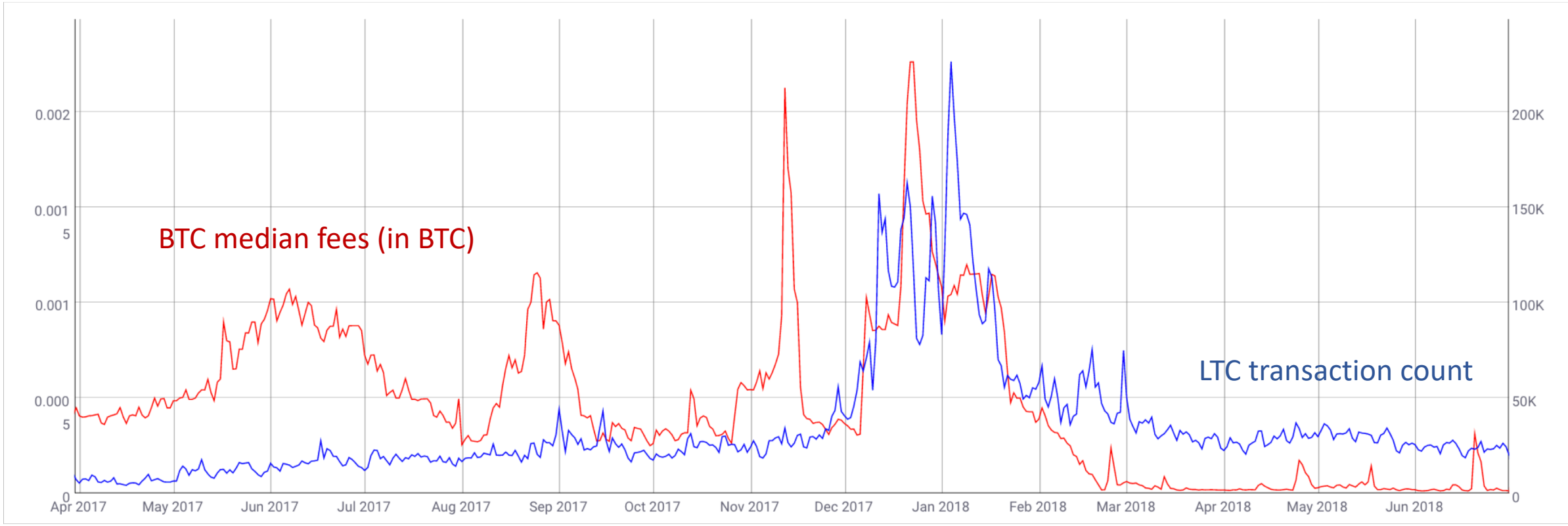
- Network effects exist; many wallets, merchants, and users are Bitcoin exclusive
- Bitcoin's settlement assurances are greater than those of other chains
- Overlay networks/some sidechains such as Lightning and Liquid are specific to Bitcoin
- Alts are more volatile and less liquid, hence more costly to transact with

No

- Clear negative feedback loop between fees and transaction count on BTC
- Cosmetically identical chains exist (LTC, BCH)
- Litecoin has been used as a Bitcoin replacement in the past
- Permanently high fees & novel low-fee blockchains might turn transactors away from BTC

Litecoin as a Bitcoin emergency spillway?

- Did fee pressure on Bitcoin induce users to transact on Litecoin instead?
- Circumstantial evidence but no clear causality



coinmetrics.io

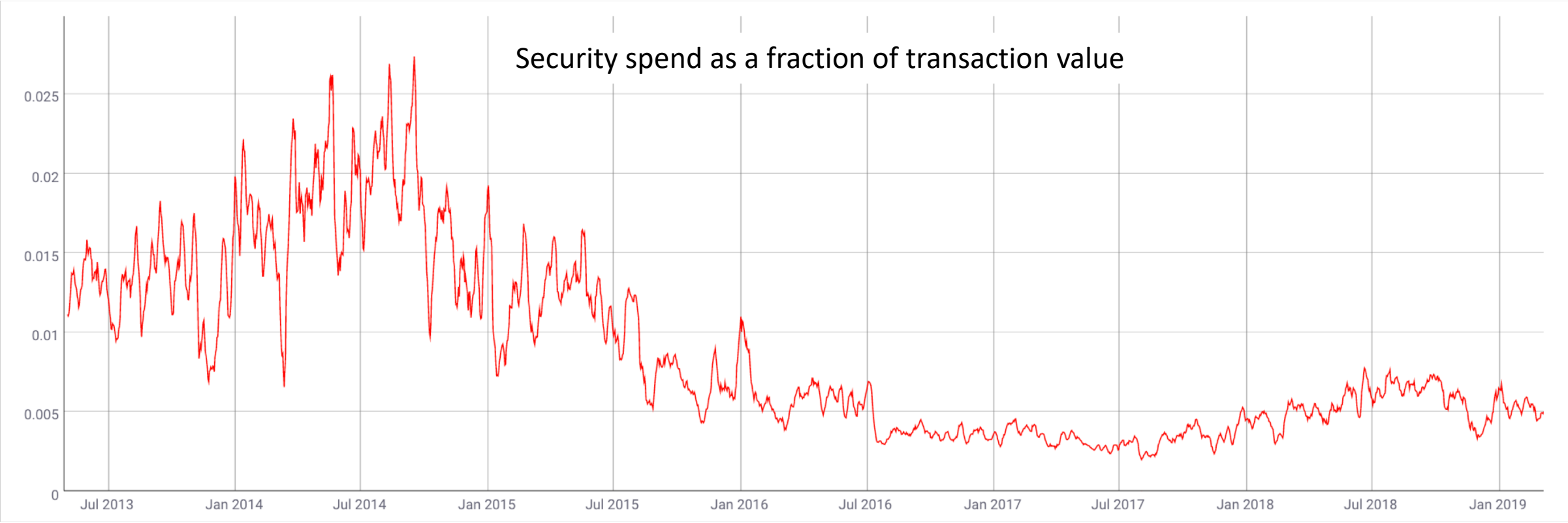
Fees are weak right now

Fees only represent ~2% of miner revenue right now!

coinmetrics.io

Daily fees are in the $150k range, annualizing to only $50m/year

How costly would a fee-only world be?



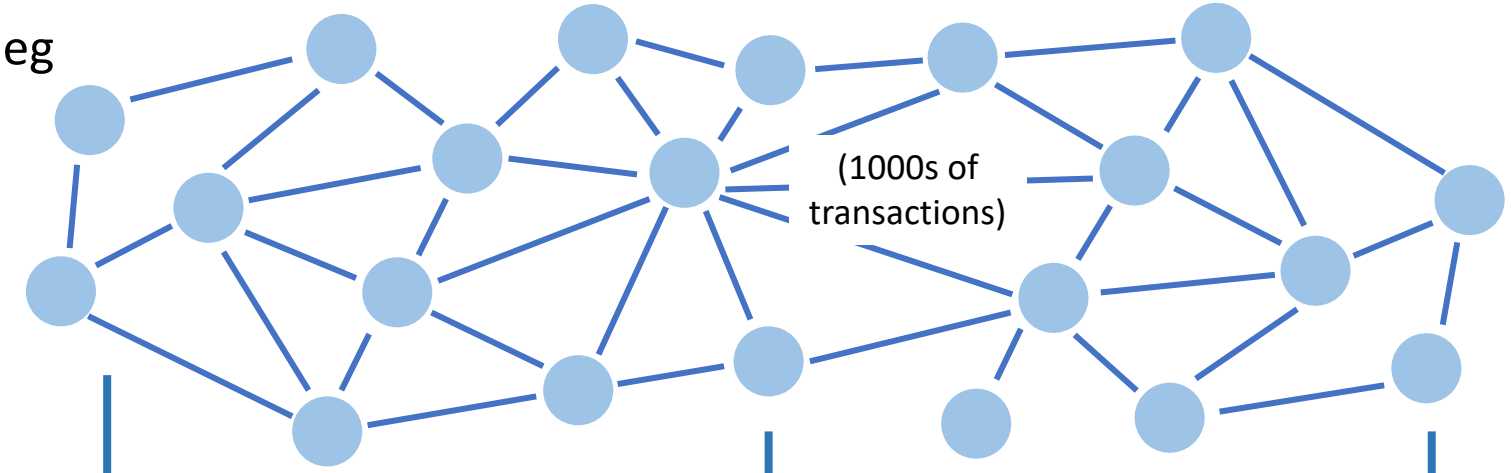
- If issuance went away today, BTC users would have to pay **0.5%** of transaction value in fees to make up the difference
- But BTC transactions are priced in bytes, not by value exchanged

Designing for long term sustainability

- Is it even appropriate to reason about enhancing fee revenues?
  - Developers tweaked the economics when they added SegWit
- Nonviable ideas: busting the 21m cap, recycling old coins, dynamic blocksize to target given fee revenue
- Potential viable: one-off blocksize contraction to induce higher fee revenue
- Simplest approach: **work to increase economic density** so people are comfortable paying meaningful fees

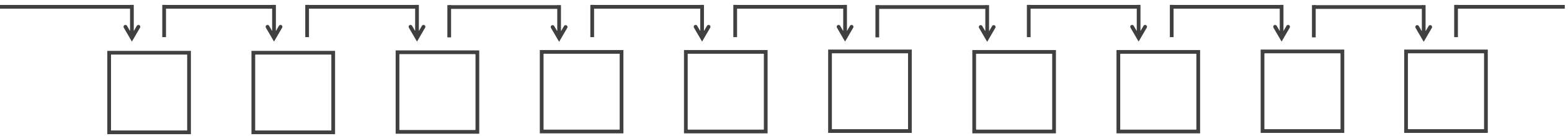
Increase economic density of transactions

Overlay network, eg Lightning



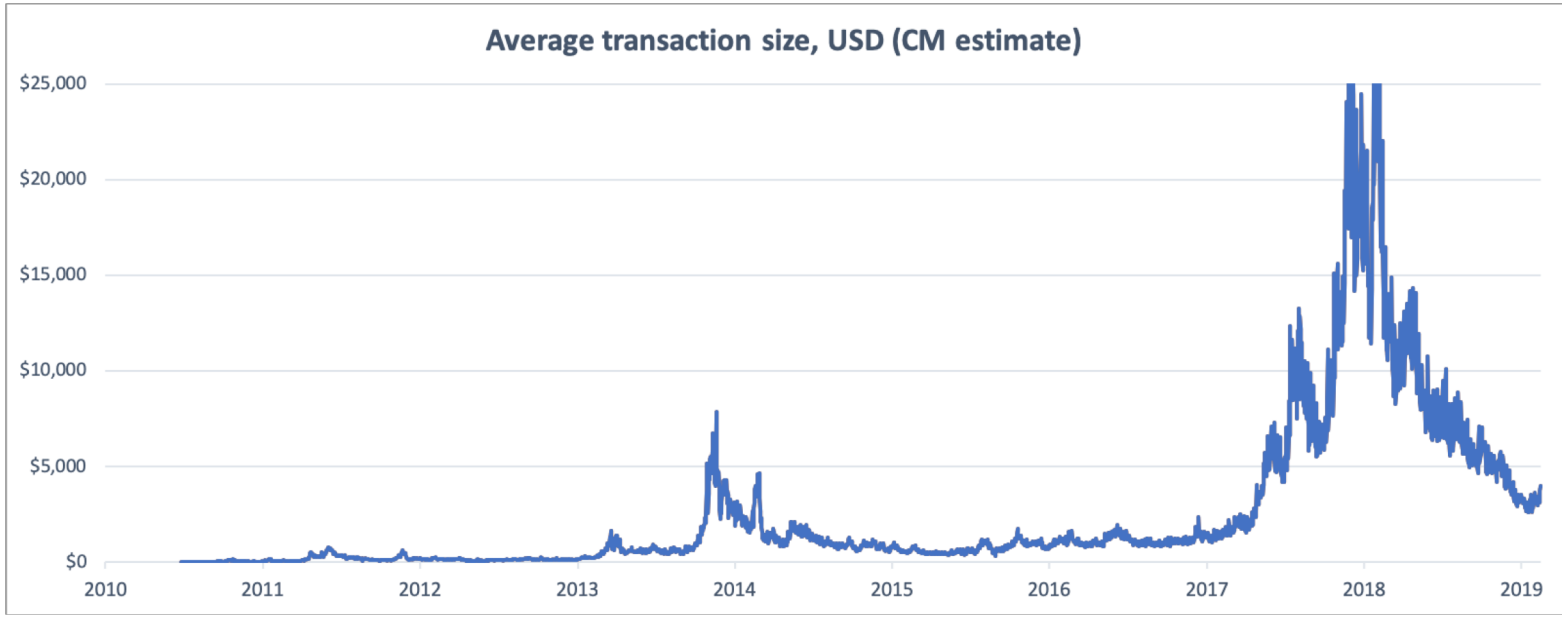
- Each transaction represents hundreds or thousands of off-chain transactions
- High fee is amortized into many 2nd layer transactions

Periodic registry to the base layer for dispute resolution & security inheritance



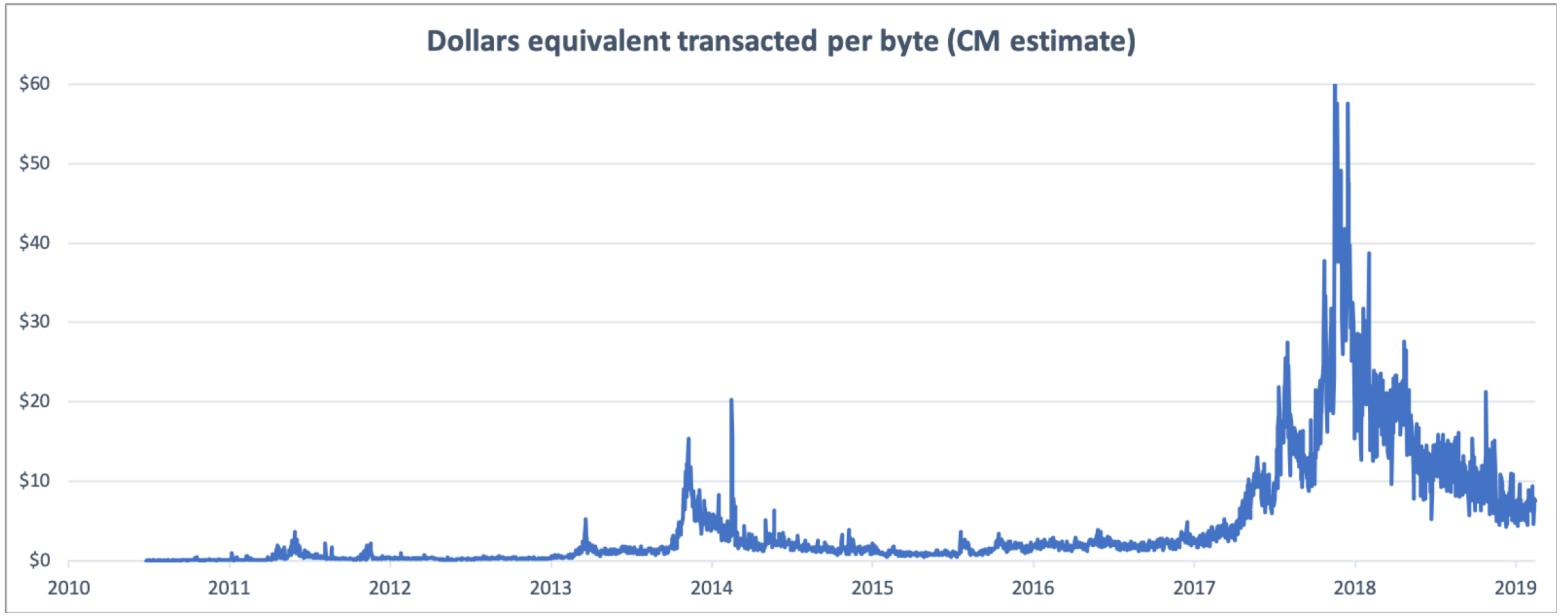
Base layer

Measuring economic density

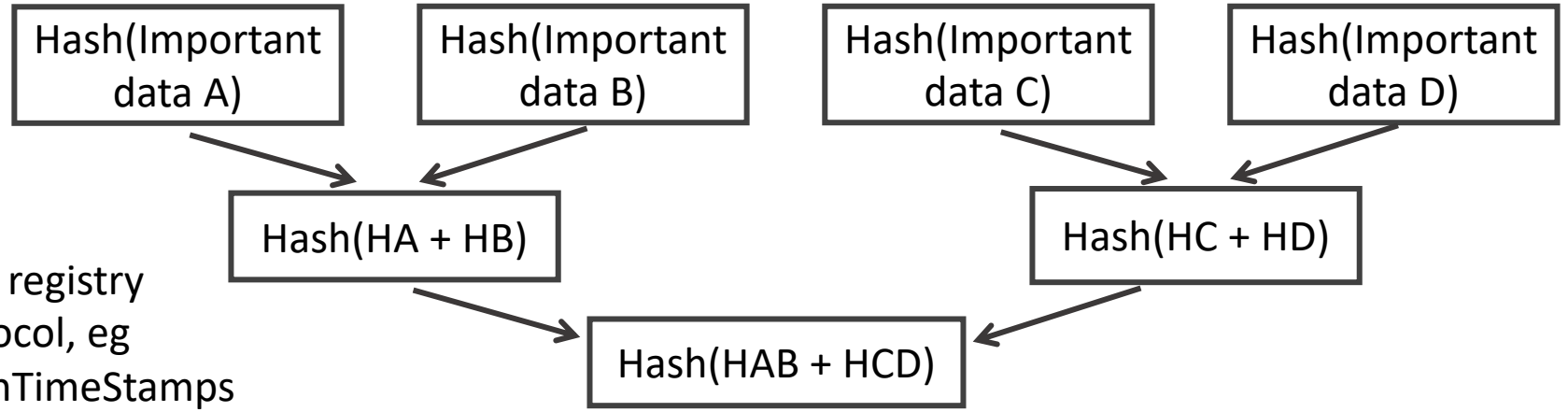


coinmetrics.io

- Average transaction size (adjusted to remove non-economic activity) peaked at $30,000, now close to $4,000
- The ultimate measure of economic density – value transmitted per byte – has declined: now around $7/byte

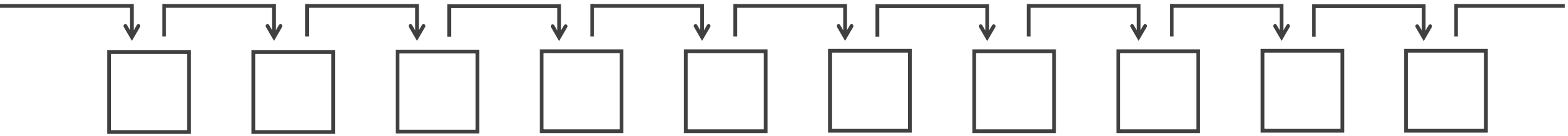


Increase semantic density of transactions



Data registry protocol, eg OpenTimeStamps

Only periodic registry required



- A single transaction can represent unbounded amounts of data
- Entities inserting meaningful data to the blockchain via a timestamping protocol might be willing to pay a non-negligible fee

Providers of semantic density in Bitcoin

Timestamping/notary

OPEN timestamps

woleet

ORIGIN STAMP

Record management

FACTOM

MONEGRAPH

blocksign

BLOCKCERTS

Assets/security inheritance

RSK

COINSPARK

BLOCKSTACK

VeriBlock

Omni

KOMODO

Other

Other merge-mined sidechains[1]

[1] See Paul Sztorc, *Security Budget in the Long Run,* Truthcoin.info

Takeaways

- Bitcoin’s dominant security model is a function of which adversarial conditions you think are likeliest to hold
- While the question of stock/flow/threshold is not settled, a mature and vibrant fee market is a requirement for long run security
- If Bitcoin block space retains a premium relative to other blockchains it is well-placed to compete in the long term
- Enhancing *semantic* and *economic* density in Bitcoin transactions is key to maximizing its long term security budget, and hence survival