Bitcoin: privacy & scale

Adam Back

Bitcoin: We are all anti-fragility

- I am speaking as an individual who cares about the success of Bitcoin
  - interested in and applied researcher in ecash individually & in startups since 1995
  - Hashcash, brands/chaum ecash library, discussions about inflation control
  - Cypherpunk list discussions about b-money/bitgold etc dating back to 1998
  - Zero-Knowledge Systems (company)Tor precursor, Brands (privacy focussed) ecash
  - Bitcoin finally figured out a deployable formula, very exciting.
- Not a bitcoin core spokesperson, developers speak for themselves
  - Developers want Bitcoin to scale and worked harder than anyone to achieve that
- Not speaking as blockstream co-founder
  - Blockstream as with any company reliant on Bitcoin wants Bitcoin to scale
  - Blockstream founders & employees all own Bitcoin and are invested in its success

What is Bitcoin? differentiators

- Bearer ecash (irreversible, unseizable, no 3rd party trust/bank)
- Permissionless, Borderless, Uncensorable
- Fungible (unfreezable, all coins universally accepted at face value)
- Privacy (or too transparent, deters use)
- Virtual commodity (Gold-like virtual mining etc)
- Non-political unlike fiat, Bitcoin is free market Internet money
  - No QE, inflation, central interest rate setting authority
- Money-like
  - Store of value ✓✓
  - Means of exchange ✓
  - Unit of account ?

Bitcoin differentiated payments

- Ask yourself “If bitcoin was down, would I not make this payment?”
- Capital controls
- Unstable / hyper-inflation
- Online use and no bank account
- Politically sensitive
- Privacy
- Grey market
- Asset protection
- Self-sovereignty (bearer ownership)

Why does decentralisation matter?

- Decentralised validation is what makes Bitcoin bearer & secure.
- Decentralised mining is how we get fungibility in Bitcoin.
- Decentralised is more survivable.
- Centralised systems can be shut-down.
- This is not hypothetical, eg government restrictions.
- Bitcoin is international & distributed, but restrictions show centralisation risk.

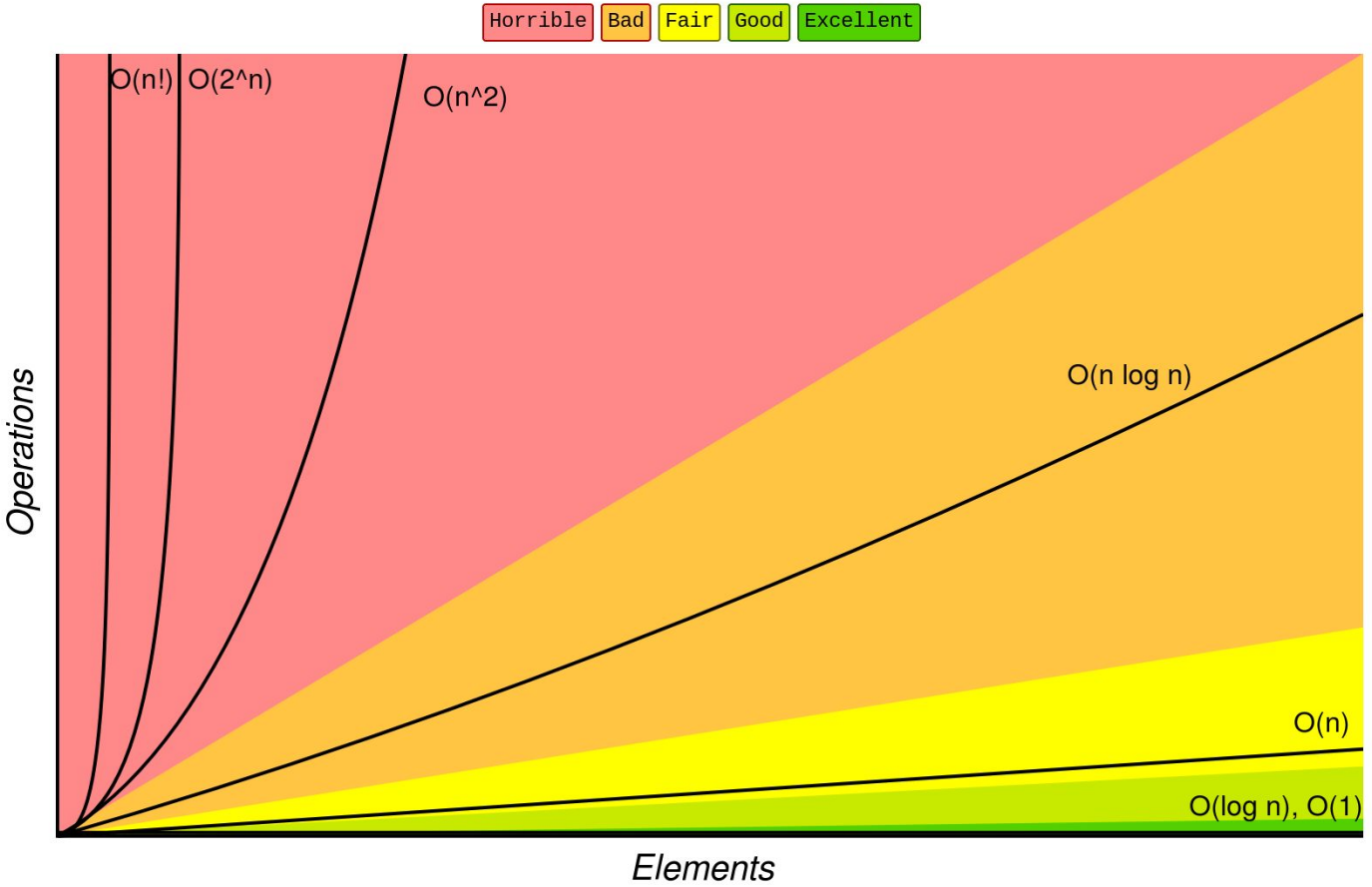
Full-nodes: Why is self-validation important?

- To be self-sovereign - to have bearer Bitcoin and not have to trust anyone
- Control your own private keys & run a fullnode. (Take good backups!)
- Fullnodes validate transactions, smartphone wallets do not (* ABcore)
- Can configure some phone wallets to connect to own node (over Tor even)
  - Greenaddress & samourai wallet have this option.
- Economic fullnodes are more useful than unused ones.
- Because you will notice and complain, and this collectively secures Bitcoin.
- Makes Bitcoin very hard to hack: have to hack all full-nodes.
- There are 100,000 user fullnodes (7,000 reachable)
- For even more privacy: use Blockstream Satellite to receive blockchain

Scaling decentralised systems is difficult

- Bitcoin is a broadcast system
- Every transaction seen by every node - like everyone sees every email!
- Network consensus is broadcast, and is slow & probabilistic (10mins+)
- If we scale it naively (increase constants) Bitcoin becomes centralised
- As resources go up Bitcoin becomes more centralised.
- it uses more resources per node reducing self-validation/eroding bearer.
- makes mining more centralised, erodes permissionlessness, fungibility.
- As Bitcoin becomes more centralised, it loses differentiating features.

Big-O Complexity Chart



Scale trade-offs: If we had to pick one?

- **A: Permissionless, uncensorable payments** - unique differentiator
- **B: Or cheap, centralised payments** - much competition for cheap payments.

- Can build less decentralised on top of centralised
- But can **not** build permissionless Bitcoin on top of centralised
- Eg medium security p2p drive-chain for retail
- Federated (multisig k of n)
- Centralised Hosted wallets

What limits scale?

- Centralisation impact limits scale.
- Limits: speed of light/latency, bandwidth costs, CPU cost.
- Validation bandwidth cost: practical for a reasonable proportion of users
- Initial sync cost (135GB and growing) 4hrs - 1day
- Keeping up 5-10GB/month
- Coin database size: 2.7GB (worse than linear lookup & cache)
- Block relaying latency: few seconds or creates orphan risk.
- Mining centralisation level. Reacts to orphan risk. Bigger pools, SPY mining.

Bitcoin ethos & change

- Bitcoin fundamentals must not change:
  - Fungible, bearer guarantee, which requires self-validation, uncensorable
  - Permissionless, unseizable, unfreezable, 21 million coin cap
- Functional requirements
  - Security, scalability, reliability, speed, uptime, backwards-compatibility etc.
- Technical consensus / IETF model
  - Improve fundamentals and functionality, while avoiding eroding other fundamentals
  - No valid technical objections unanswered
- Opt-in preferred
  - An opt-in feature of value to many, that does not detract from people who do not use.

Bitcoin satellite backbone - global access

45cm KU band dish

USB computer interface

bi-directional internet

Satellite for resilience

- Internet connections sometimes fail
- Network splits / undersea cable failure
- Satellite is a secondary network
- Also better privacy as passive
- Cheaper no recurring cost to receive
- Build infrastructure in emerging markets
- Uplink via SMS or bidirectional satellite (expensive but transactions are small)

Short-term scale

- Segwit
- Best practices:
  - Fee estimation
  - Batching
  - change consolidation
- Lightning
- Lightning factories (v2)
- payment-channels
- netting

Mid-term scale

- More network compression
- Pre-consensus (pre-distribute block proposals)
- Lower latency network infrastructure
- Hard-fork: https://bitcoinhardforkresearch.github.io/
  - Spoon-net & others (Johnson Lau, Luke Dashjr)
- Drive-chain (medium security side-chain Paul Sztorc)
  - Slow return security mechanism
  - Incentive questions
  - secondary scale limits if have to val
- Lightning v2 (R&D topics)

Longer-term scale

- Unilateral withdraw from semi-decentralised chains
- Chain security funding questions long term after more halvings
  - Bottlenecks are security & latency today
- SNARKs / STARKs
  - Much more efficiency needed, but new area with active R&D, and computers get faster
  - Signature of program execution - if the program is the blockchain validation
  - Then dont need to see the data