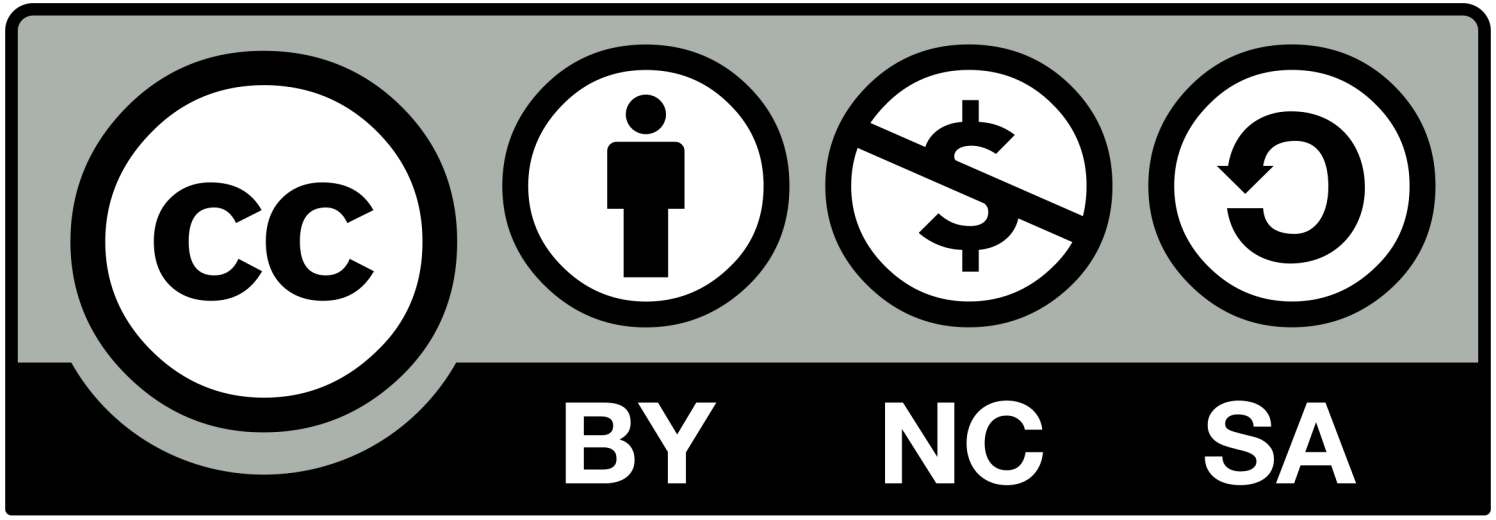
The Next Challenges of Bitcoin

HOW TO MAKE THE DECENTRALIZED ALTERNATIVE TO THE FINANCIAL SYSTEM SUCCEED?

Stéphane Roche

2019-02-02

CREATIVE COMMONS



ABOUT STEPHANE

2015

Work at Ledger - hardware wallet company

2016–2017

Work on Ethereum

- Learn and play
- Co-found non-profit organization Asseth
- Contribute to the ERC20 Consensys smart contracts
- Dether.io

2017–2019

Found Bitcoin Studio

Focus on Bitcoin education

Consultant at Chainsmiths

https://www.bitcoin-studio.com
@janakaSteph on Twitter
bitcoin-studio@protonmail.com

OUTLINE

1. Mining, fee market
2. Lightning Network
3. Digital signature algorithms, QC threat
4. Privacy
5. Education, contribution

RETROSPECTIVE

- Bitcoin Core contributors did an amazing job so far, optimizing without introducing consensus bugs

- Segregated Witness (virtual blocksize increase, faster signature verification, script versioning)
- Lightning Network

- Soft fork deployment methodology (BIP34, BIP9, BIP91, BIP148, BIP8)
- Libsecp256k1 heavily optimized and protects against specific attacks
- Pruning (discard old data and enjoy the exact same security of running a full node)
- Multiwallet (completely segregated wallets on the same node)
- Cory Field's net refactor (efficient block/transaction propagation)
- Groundwork for process separation (Russ Yanofsky)
- Fee estimation improvements (Alex Morcos)
- Better multi-threading (reducing global locks, Matt Corallo)
- ...

DECENTRALIZING MINERS PRODUCTION

- Semiconductor foundries (TSMC, Samsung)
- Miners manufacturers (Bitmain, Halong Mining, GMO miner)
- Information asymmetry between manufacturers and customers
- Mining market is just starting to mature

MINING DECENTRALIZATION

- Bitcoin mining landscape has many pressures that encourage centralization
- Current most widely deployed mining protocol Stratum is very bad
- We need a more diverse body of miners constructing block templates
- BetterHash BIP by Matt Corallo
  - Drastically increases effective mining decentralization by separating Work and Payout protocols
  - Removes network-level centralization attacks pools can do
  - Pools still in full control of payout management and variance reduction
- To further develop decentralized mining pools like P2Pool
  - Chris Belcher suggested a scheme using Lightning Network

SMARTER FEE MARKET

- To further develop a smarter fee market to subsidize the block reward
  - We can’t rely on the price doubling every 4 years
  - Not enough mining reward could make mining more centralized
- Current fee market does not maximize miners revenue when blocks are not congested
- Lavi, Sattath and Zohar suggested Monopolistic Price Mechanism and Random Sampling Optimal Price Mechanism

LIGHTNING NETWORK

- Bitcoin has choosen to bet on layer 2 in order to scale

- Many technical challenges
  - Channel monitoring (watchtower)
  - Routing
  - Atomic Multi-Path Payments
  - Splicing (BIP118)
  - Multi-hop locks

DIGITAL SIGNATURE ALGORITHMS

- Current focus is on replacing ECDSA for EC-Schnorr algorithm (MuSig)

- More efficiency, privacy, functionality
  - Key aggregation (multisig)
  - Signature aggregation (reduce the signatures in a tx to one or a few)
  - Batch validation (all or nothing)
  - Improve privacy (private multisigs, incentive to use CoinJoin, ...)
  - Provably secure (ECDSA is not)

- Not quantum-resistant (same ECDLP assumption)

- Lot of new developments rely on Schnorr (Taproot, Scriptless scripts, DLC, privacy, ...)

QUANTUM COMPUTING THREAT

- Over-hyped topic

- Quantum skepticism
- Most optimistic estimates states that ECDSA could be broken in 2027

- Potential solutions in blockchain context
  - Hash-Based cryptography (OTS, Winternitz OTS, FTS, HORS, LMS, XMSS, SPHINCS)
  - Lattice-Based cryptography (BLISS, DILITHIUM, NTRU, ...)

PRIVACY

- Privacy and fungibility are essential properties of sound money
- To further develop mixing protocols
  - CoinJoin, CoinShuffe, CoinShuffe++, ValueShuffle, ZeroLink – Wasabi wallet
- Confidential Transactions (Elements) with Bulletproof
- Private transaction broadcasting (Tor, Dandelion, Dandelion++)
- Private transaction retrieval in light clients
  - Bloom filter leaks too much information
  - Compact Client Side Filtering (Neutrino)
- Private smart contracts (MAST) with Taproot / Graftroot

EDUCATION

- Quite a lot to learn
  - Cryptography
  - Key management
  - Game theory
  - Computer science
  - P2P networking
  - Hardware, system administration
  - Consensus algorithms, mining, energy
  - Economics, finance
  - Marketing, scams
  - ...

- Highschool should prepare people for Bitcoin

OPEN SOURCE CONTRIBUTION

- Bitcoin is an open source project
  - It is a community effort
  - We need everyone
  - Donation

CONCLUSION

- Bitcoin did an amazing job so far, but the battle is far from being won
- « Blockchain not Bitcoin » cannot succeed
- This is still an experimental technology
- Each one of us is invited to contribute in his capacity
- Each of these challenges is a business opportunity