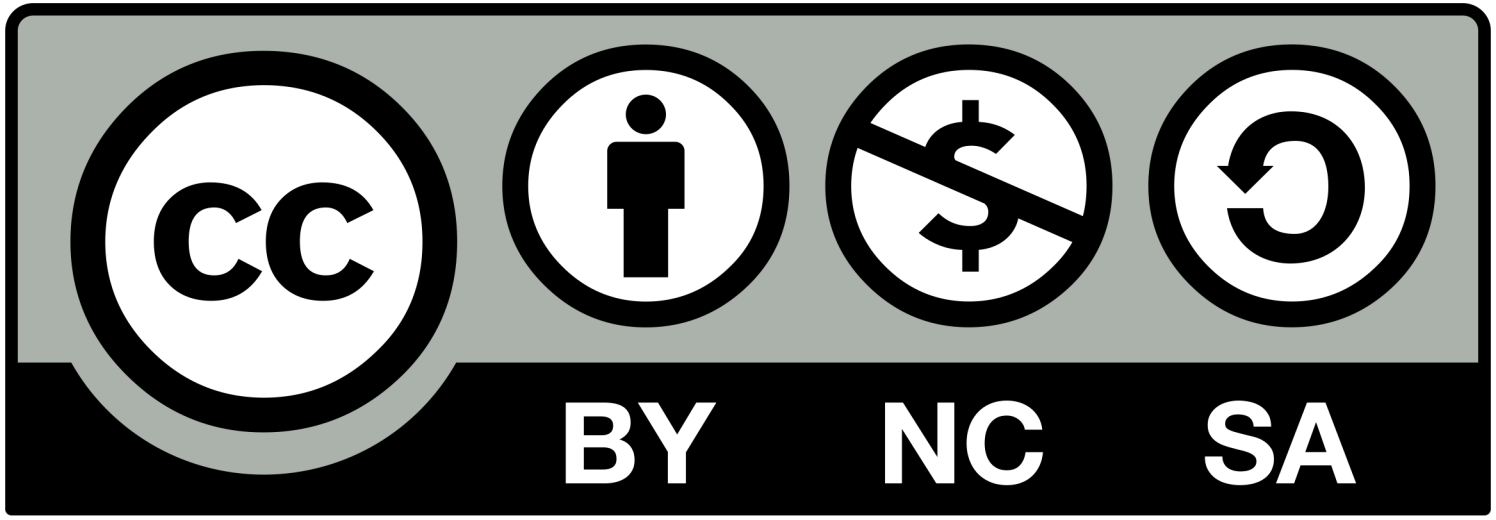
The Beginning of Your Blockchain Journey

OR WHY BLOCKCHAIN IS HARD TO UNDERSTAND

Stéphane Roche

2018-08-12

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

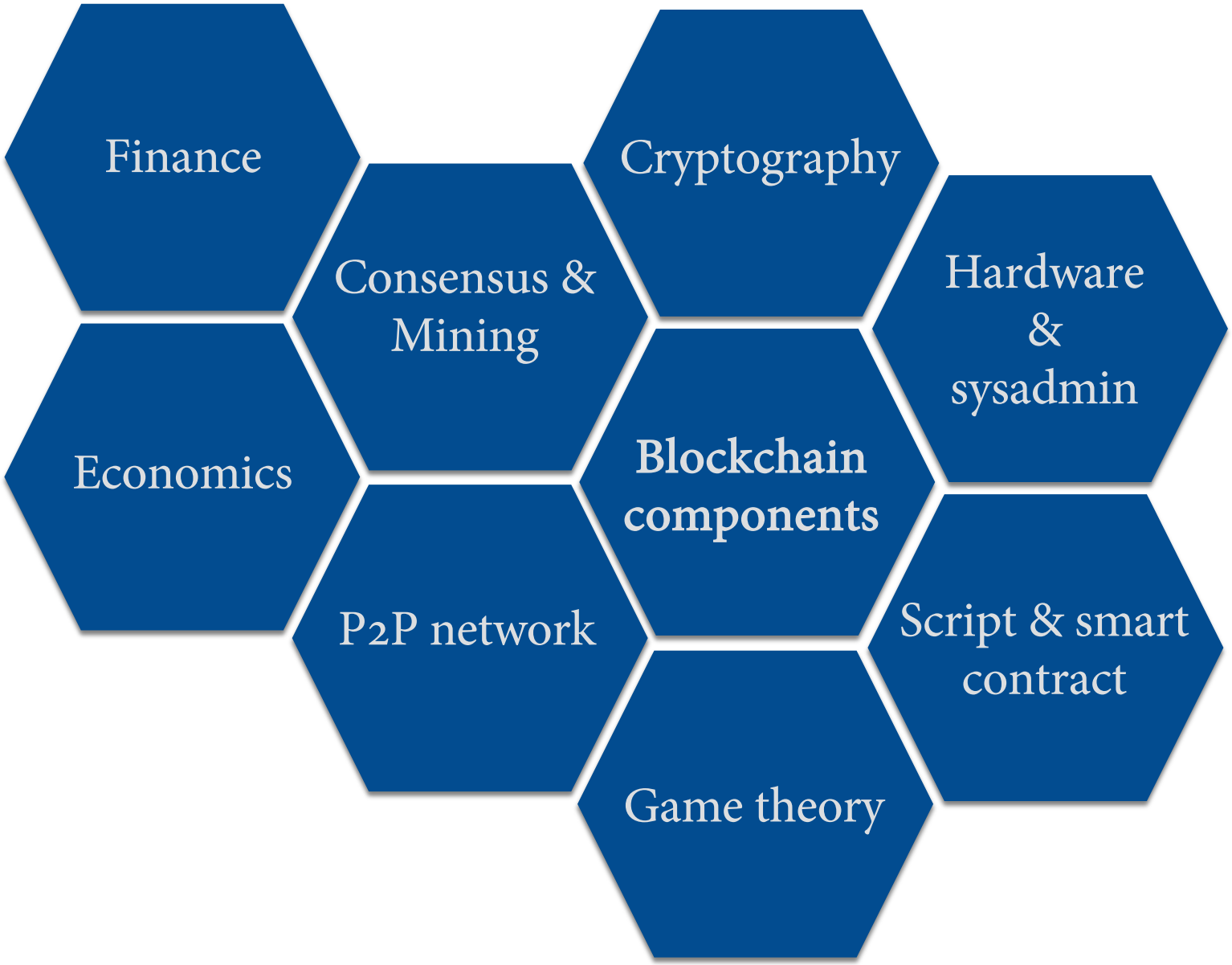
Consultant at Chainsmiths

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

WHAT IS BLOCKCHAIN?

- A « database » with specific rules about how to insert data

- It cannot conflict with some other data (consistent)
- It’s append-only (immutable)
- The data itself is locked to an owner (ownable)
- It’s replicable and available
- Everyone agrees on what the state of the things are (canonical)
- It works without a central party (decentralized)


Finance
Cryptography
Consensus & Mining
Hardware & sysadmin
Economics
Blockchain components
P2P network
Script & smart contract
Game theory

YOU SHOULD START WITH BITCOIN

- Most mature technology, project
  - And still very experimental
  - Many talented developers and cryptographers
  - Many projects have copy many parts of Bitcoin
- Simplest design and still complex
- The whole cryptomarket has been built around Bitcoin
- It is impossible today to be an expert in more than one blockchain
- Has proven not to be a scam
  - Do your own research, be skeptical

CRYPTOGRAPHY

- Blockchains work mainly thanks to cryptography
  - I would recommend to start learning blockchain by cryptography
  - History and fiction books are a pleasant way to learn classical cryptography

- Bitcoin originates from the community of independent cryptographers and cypherpunk movement
  - So modern cryptography history is important to really understand Bitcoin

- Cryptographic algorithms are hard to design and implement properly
  - New cryptography must be tested in the wild

- No “complex” cryptography in Bitcoin (for now...)
  - Many hash functions everywhere
  - Some key derivation functions
  - ECDSA for authentication
  - No encryption
- A lot of new cryptography is coming
  - Privacy schemes, more complex scripts, new signature algorithm, ...
- Other blockchain like Zcash and Monero are much more complex (ZKP, Ring signature)
- You should be skeptical towards any blockchain team that have a poor understanding of cryptography

CRYPTOGRAPHY BIBLIOGRAPHY

- The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2000, Simon Singh

- Cryptography: A Very Short Introduction, 2002, Fred Piper, Sean Murphy

- New directions in cryptography, 1976, Whitfield Diffie, Martin E. Hellman

- Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th Anniversary Edition, 2015, Bruce Schneier

CONSENSUS & MINING

- Consensus/mining is the most distinctive component of blockchain

- Consensus rules, enforced by the mining process, using a consensus algorithm

- Proof of Work is the most tested blockchain consensus algo
- Other consensus algos are very experimental
- Consensus algos are much easier and effective on private blockchains

CONSENSUS & MINING BIBLIOGRAPHY

- https://blog.bitmex.com/mining-incentives-part-1-the-difficulty-adjustment-and-mining-profits/
  - Mining Incentives – Part 1 – The Economics of the Difficulty Adjustment

- https://www.youtube.com/watch?v=sE7998qfjgk
  - Andreas M. Antonopoulos: "Consensus Algorithms, Blockchain Technology and Bitcoin"

GAME THEORY

- Used in the context of mining (pool mining in practice)
- Tightly related to economics
- Hard discipline to learn because a lot of maths and specific vocabulary

- Lot of known attacks in PoW systems
  - Selfish mining
  - Miner bribery
  - 51% attack
  - Pool cannibalization
  - Stubborn mining
  - DoS of competing miners

- Lot of new attacks in PoS and others

- Cryptoeconomics, the blockchain mechanism design
  - Designing economic mechanisms or incentives, toward desired objectives, in strategic settings, where players act rationally
  - Blockchain allows us to build tailor-made economic mechanisms

- Not enough academic research on game theory in blockchain

GAME THEORY BIBLIOGRAPHY

- The Bitcoin Mining Game, 2016, Nicolas Houy

- https://www.youtube.com/watch?v=UPxaCj8ZsEU
  - Game Theory & Network Attacks: How to Destroy Bitcoin, Max Fang & Philip Hayes

- https://thecontrol.co/cryptoeconomics-101-e5c883e9a8ff
  - Cryptoeconomics 101, Nick Tomaino

- https://cesc.io/
  - Crypto Economics Security Conference
  - Oct 15-16 2018, UC Berkley

- Vitalik Buterin, Vlad Zamfir talks and blog posts

SCRIPTS & SMART CONTRACTS

- Bitcoin allows to compose a script from opcodes
  - Language is not hard but lack of developer tools

- Smart contracts platforms use common programming languages or specific ones
  - Need much more research on formal methods/safety engineering
  - Code upgrade is tricky
  - Should not be used by inexperienced developers

HARDWARE AND SYSADMIN

- You are supposed to setup your own fullnode
  - Requires sysadmin/Linux skills

- PoW mining is a fierce technical competition

- Semiconductor / Application-Specific Integrated Circuit
  - 7nm chip announced
  - Immersion cooling
  - Quick access to the newest chips is crucial
  - We are observing new Bitmain competitors (Halong Mining, GMO Internet)

- Mainnet Bitcoin Lightning Network is improving quickly

- Ethereum
  - Infura centralized service provides Ethereum access to a lot of projects
  - The minimum specs are already high, nodes harder to synchronize

HARDWARE BIBLIOGRAPHY

- https://irds.ieee.org/
  - International Roadmap for Devices and Systems

P2P NETWORK

- Nodes randomly connect to other nodes
  - Needs DNS seeds to bootstrap peer discovery
- Routing in Lightning Network is a hot topic today
  - Routing layer is independent of LN
  - There is a lot to create and experiment with
- Relay networks to speed up block propagation for miners
  - FIBRE (Fast Internet Bitcoin Relay Engine)
  - Fast Relay Network, Falcon

ECONOMICS

- Decentralized, open source, permissionless, censorship-resistent digital currency is a real revolution
  - A cryptocurrency project needs time to be decentralized
  - ICO coins are heavily centralized
  - A coin can starts being a security and becoming a commodity
- Bitcoin has a fixed number of coins, issuance is halved every four years
- Useful to assess native coin issuance models and ICOs

ECONOMICS BIBLIOGRAPHY

- The Bitcoin Standard: The Decentralized Alternative to Central Banking, 2018, Saifedean Ammous

FINANCE

- The cryptomarket is getting big (venture capital, investment funds, ETF, big banks, stock exchanges, ...)
- Regulation, SEC reports, ...
- Cryptoasset valuation is a new field
- Technical analysis (how to read a trading chart)
  - The price influences the news (not the other way around)
- Portfolio/risk management

- The big challenge in this field is to build reliable and efficient decentralized non-custodial exchanges
  - Trusted gateway (Waves)
  - Trusted execution engine (Tesseract with Intel SGX)
  - Trusted third party (BitGo)
  - Blockchain (Lightning, 0x, Commonwealth Crypto, ...)

- Off-chain txs
- Atomic swapes trades
- Multisignature txs / escrows

FINANCE BIBLIOGRAPHY

- The New Trading for a Living: Psychology, Discipline, Trading Tools and Systems, Risk Control, Trade Management, 2014, Alexandre Elder

- Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond, 2017, Chris Burniske

CONCLUSION

- Blockchain is at the crossroad of many disciplines, hard to get the big picture
- You can’t understand a complex technology without any CS skills
  - A background in cryptography is essential
- But you can understand the purpose of this technology
  - Open, censorship-resistant, immutable ledger
  - For value transfer, anchoring, code execution
- A blockchain is a living evolving organism
  - Collecting data is important to understand how it behaves under different circumstances (pragmatic methodology)