Blockchains: Proof-of-What?

Louis Abraham

About me

Louis Abraham

louis.abraham@yahoo.fr

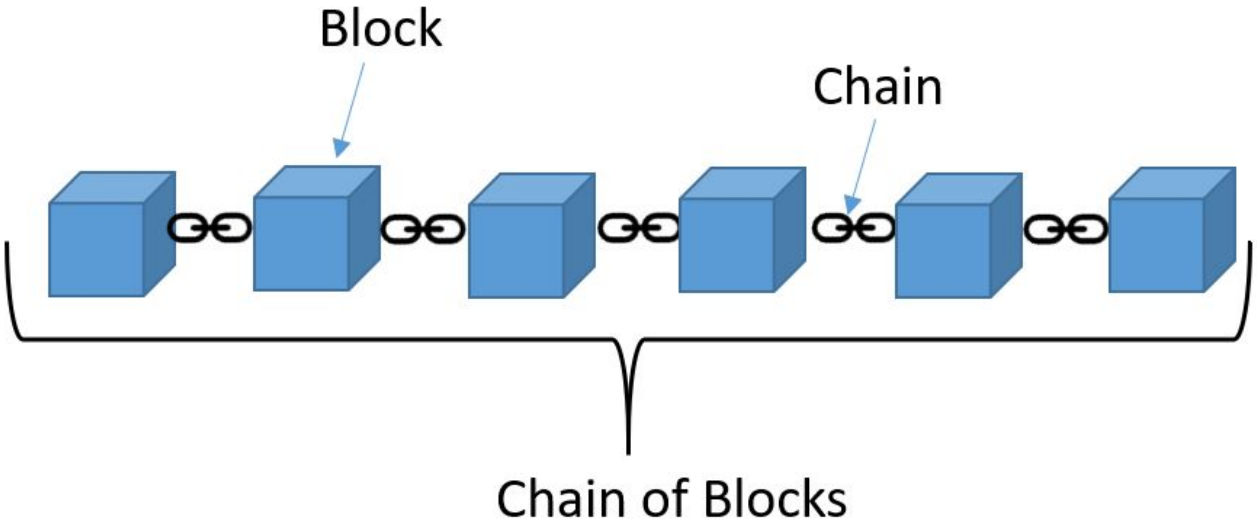
Graduate from École polytechnique and ETH Zurich

Currently :

- Secrecy (https://secrecy.me/)
- Gematria Technologies (https://gematria.tech/)

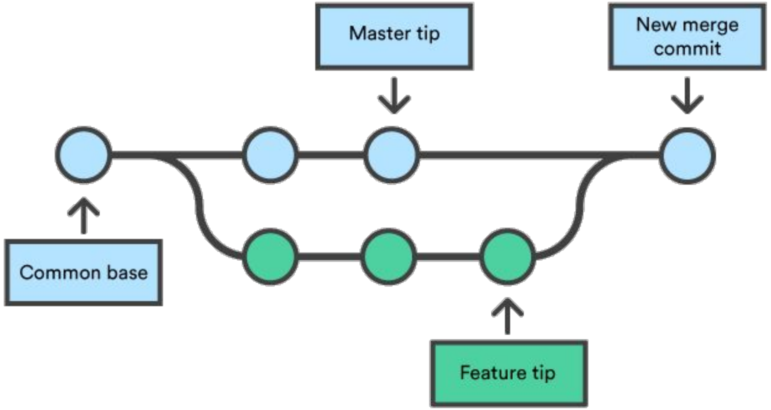
What is a blockchain?

- “chain” of “blocks”



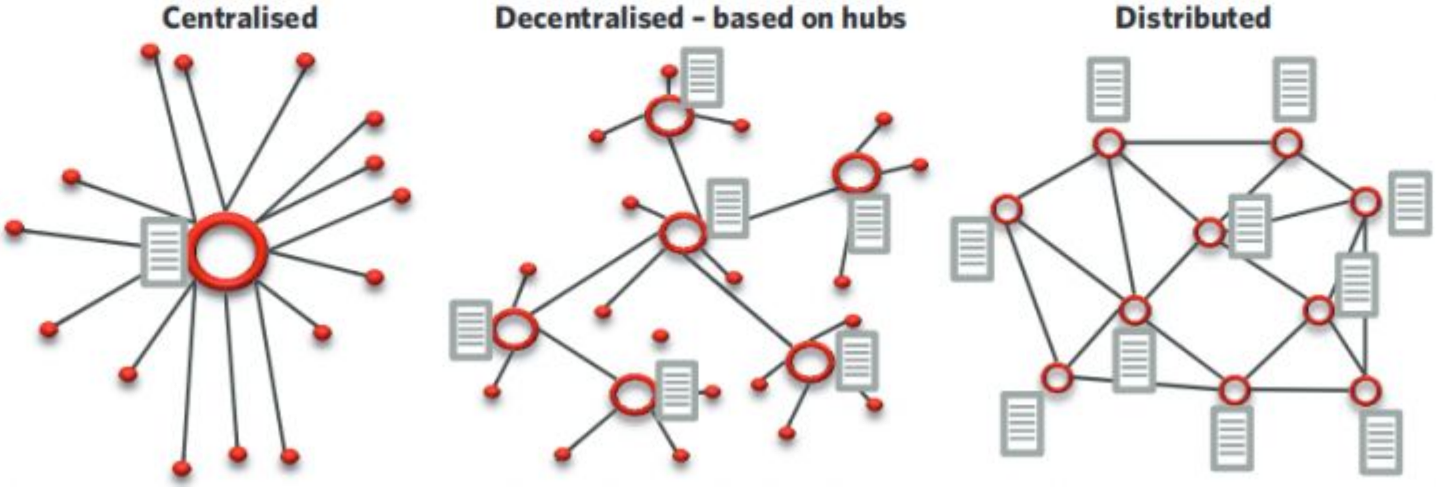
Is git a blockchain?

- git is a distributed version control system
- git groups modifications in “commits” (~blocks)
- each commit is linked to a parent commit, identified with a hash



A definition of blockchain

- ***distributed ledger*** *that is organized in chains*
- nobody cares about blockchain per se, what really matters are DLT



Public blockchains

- most examples are cryptocurrencies (Bitcoin, Ethereum)
- Total market cap: 450B€
  Including 300B€ for Bitcoin and 50B€ for Ethereum

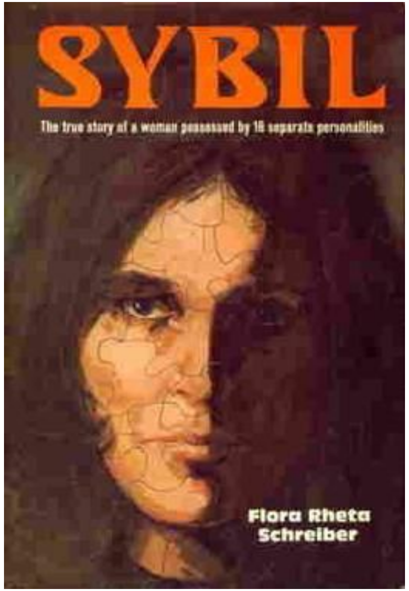
- Why are most public blockchains cryptocurrencies?
  Because nobody works for free!

How do you create tokens?

- In most systems: tokens are created (mined) by validators
- Notable exception: in Ripple (XRP), 100M tokens were created.
- Ripple is a DLT but **not** a blockchain!

How do you achieve consensus?

- Many consensus algorithms!
- Need to prevent Sybil attacks


SYBIL
The true story of a woman possessed by 16 separate personalities
Flora Rheta
Schreiber

How to prevent Sybil attacks?

Consensus is not the same as Sybil mitigation

- Proof-of-Work: used in all major blockchains
- ??? (see after)

What is Proof-of-Work?

- kill three birds with one stone: consensus, sybil attacks and money creation
- Proof-of-work is really just a **lottery**
- A ticket is bought by computing to solve a hard problem (mining)
- The first one who solves the problem can decide what the next block is

Why does everybody want to replace proof-of-work?

- Bitcoin consumes 60-100 TWh per year

  -> Equivalent to a median European country
- High variance of rewards
- Almost no penalty if people cheat (no slashing)
- Security depends on the hashrate and the currency cost

  -> how much would it cost to own 51% of the network for a few hours?
- Game-theoretic flaws (e.g. selfish miner)
- Centralized: top 4 (resp 3) miners in Bitcoin (resp Ethereum) possess more than 51% of the computing power
- High transaction cost and latency

Alternatives to PoW

- Proof-of-Stake : cheaters are punished with a slashing mechanism
- Proof-of-Authority : “Proof of Stake model that leverages identity as the form of stake rather than actually staking tokens”.

In practice

- Ripple can be considered to use Proof-of-Authority
- Libra was a Proof-of-Authority project

- Proof-of-Stake: many projects, none really gained traction
- **Ethereum 2.0**: scheduled since 2015, delayed since 2016
  - **Launched a first phase on December 1st!**
  - will use Proof-of-Stake
- Major issue of Proof-of-Stake: online exchanges

Is Sybil mitigation really a challenge?

- KYC and AML policies are pushing digital identity forward
- Sybil mitigation is not necessary if you have digital identity

Questions?

Slides will be available at https://louisabraham.github.io/