Stochastic Models for blockchain analysis

Introduction

Pierre-O. Goffard

Institut de Science Financières et d'Assurances
pierre-olivier.goffard@univ-lyon1.fr

5 septembre 2021

Blockchain

A data ledger made of a sequence of blocks maintained by a achieving consensus in a Peer-To-Peer network.

- Decentralized
- Public/private
- Permissionned/permissionless
- Immutable
- Incentive compatible
  - The nodes are compensated for their hard work in cryptocurrencies

We will focus on public blockchain and their associated consensus protocol.

Blocks

A block contains

- block height/ID
- Time stamp
- hash of the block
- hash of the previous block
- Set of transactions (data stored in the blockchain)

```
Block Height: 0
Block Hash: a52bea61a9f4131588cc101e8e1c731fa9f69f16934c5ab3a05a2134a42c13e0
Time:2021-07-12 10:03:04.812744
Block data: [{'sender': 'Coinbase', 'recipient': 'Satoshi', 'amount': 100, 'fee': 1}]
Mined: False
Previous block hash: 0
--------------
```

Cryptographic Hash function

A function that maps data of arbitratry size (message) to a bit array of fixed size (hash value)

$$h : \{0,1\}^* \mapsto \{0,1\}^d.$$

A good hash function is

- deterministic
- quick to compute
- One way
  - ↪ For a given hash value $\overline{h}$ it is hard to find a message m such that

$$h(m) = \overline{h}$$

- Colision resistant
  - ↪ Impossible to find m_1 and m_2 such that

$$h(m_1) = h(m_2)$$

- Chaotic

$$m_1 \approx m_2 \Rightarrow h(m_1) \neq h(m_2)$$

Consensus protocols

The mechanism to make all the nodes agree on a common data history.

The three dimensions of blockchain systems analysis

1. Efficiency (Queueing theory)
   - Throughputs
   - Transaction confirmation time
2. Decentralization (Entropy)
   - Fair distribution of the accounting right
3. Security (Insurance Risk Theory)
   - Resistance to attacks

X. Fu, H. Wang, and P. Shi, "A survey of blockchain consensus algorithms : mechanism, design and applications," *Science China Information Sciences*, vol. 64, nov 2020.

Proof of Work

The nodes compete to solve a cryptographic problem by brute force search.

PoW

1. Draw a random number (nonce)

$$X \sim \{1, \ldots, 2^{32}\}.$$

2. While $X > L$, where L is the target then try again

Nodes are chosen according to their computing power

S. Nakamoto, "Bitcoin : A peer-to-peer electronic cash system." Available at https://bitcoin.org/bitcoin.pdf, 2008.

Proof of Stake

PoW is slow and ressource consuming. Let $\{1,\dots,N\}$ be a set of miner and $\{\pi_1,\dots,\pi_N\}$ be their share of cryptocoins.

PoS

Node $i \in \{1,\dots,N\}$ is selected with probability π_i to append the next block

Nodes are chosen according to what they own.

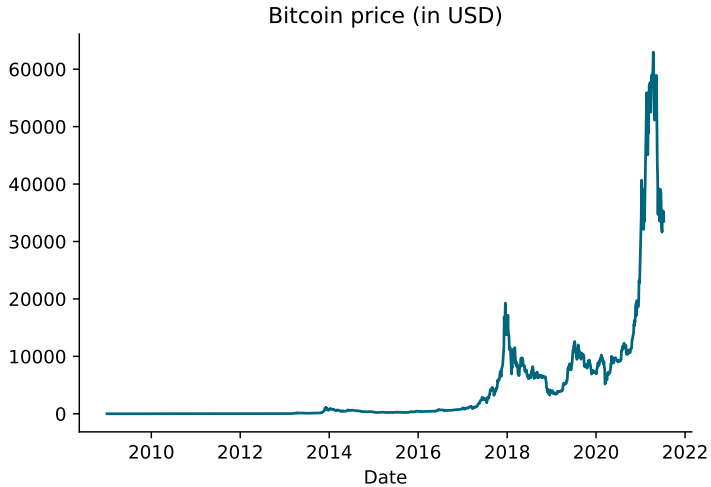
- Nothing at stake problem
- Rich gets richer ? (To be discussed later on)

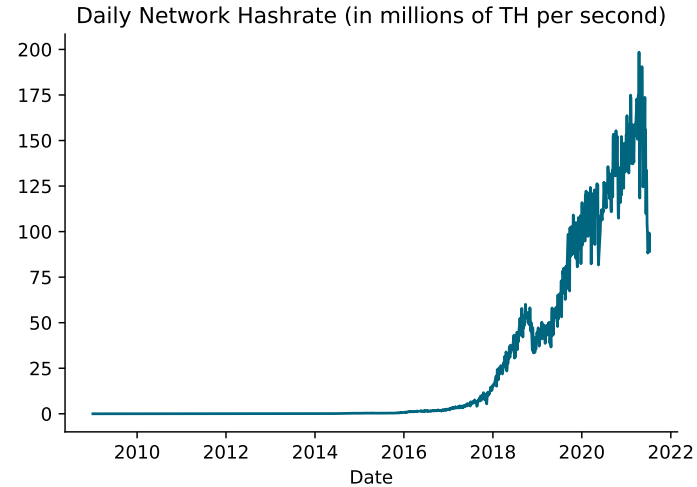
F. Saleh, "Blockchain without waste : Proof-of-stake," *The Review of Financial Studies*, vol. 34, pp. 1156–1190, jul 2020.

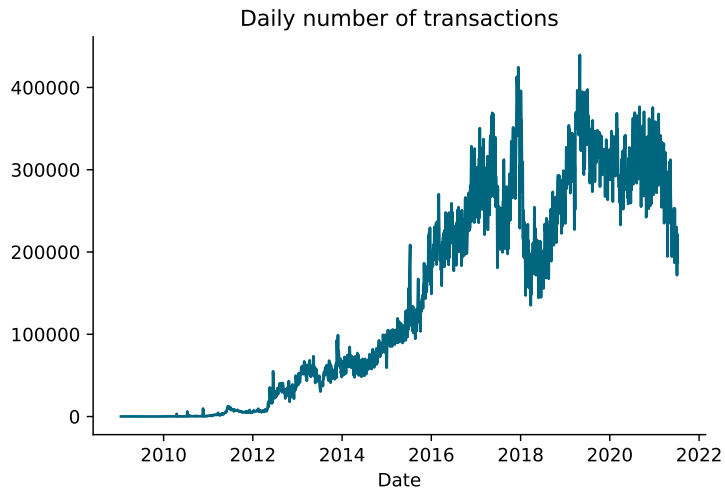
Applications of blockchain : Cryptocurrency

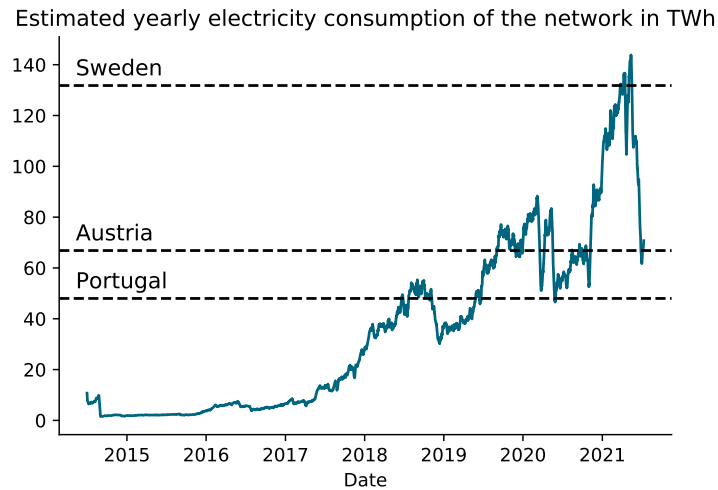
S. Nakamoto, “Bitcoin : A peer-to-peer electronic cash system.” Available at https://bitcoin.org/bitcoin.pdf, 2008.

- Transaction anonymity
- Banking and reliable currency in certain regions of the world
- Money Transfer worldwide (at low fare)
- No need for a thrusted third party









. **Sources** : `https://www.blockchain.com/` & `https://cbeci.org/`

Decentralized application

The network provide ressources such as

- storage
- computing power

through a smart contract on the ethereum blockchain.

GOLEM (`https://www.golem.network/`)

Build a network of idle computers to do paralell computing.

Utility tokens are used to access the service and provision the network ressources.

Equation of Exchange (Fisher 1911)

$$MV = PQ$$

Decentralized finance

DEFI creates new financial architecture

+ Non custodial
+ Anonymous
+ Permisionless
+ openly auditable

- Unregulated
- Tax evasion
- Fraud
- Money laundering

Extends the Bitcoin promises to more complex financial operations

- Collateralized lending
- Decentralized Exchange Platform
- Tokenized assets
- Fundraising vehicle (ICO, STO, ...)

S. M. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. J. Knottenbelt, "Sok : Decentralized finance (defi)," 2021.

Decentralized insurance

Parametric insurance

Compensation if a measurable quantity reaches a threshold

- Example : Flight delay insurance
  - `https://etherscan.io/address/0xdc3d8fc2c41781b0259175bdc19516f7da11cba7`
- Use smart contract and off-chain data through oracles
- Transparent and automatic

Another example is P2P insurance.