

Stochastic Models for blockchain analysis

Introduction

Pierre-O. Goffard

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

28 septembre 2021

BFS summer school

Mini course of four lectures on the topic of blockchain at the 1st Bachelier Finance Society Summer school.

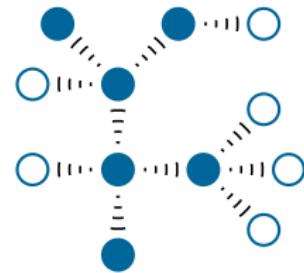
- Link to the event <https://www.bachelierfinance.org/09-2021>
- Link to the course material
<https://pierre-olivier.goffard.me/BLOCKASTICS/>



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



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 arbitrary 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 \bar{h} it is hard to find a message m such that

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

- Collision 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)

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

- 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 trusted third party

How does it work ?

- 1 No central authority (Decentralized network)
- 2 Ledger to record all the transactions and coin ownership (blockchain)
- 3 A coin generation process (block finding reward)
 - Incentive to the full nodes
- 4 Ownership can be proved cryptographically (wallet associated to a public/private key)
- 5 Transactions can be issued by an entity proving ownership of the cryptographic unit (through the private key)
- 6 The system cannot process more than one transaction associated to the same cryptographic unit (double spending)



J. Lansky, "Possible state approaches to cryptocurrencies," *Journal of Systems Integration*, vol. 9, pp. 19–31, jan 2018.

Cryptocurrency implementation

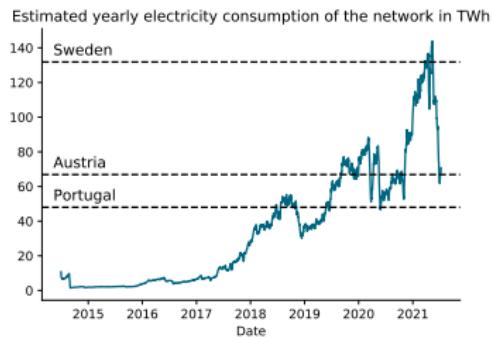
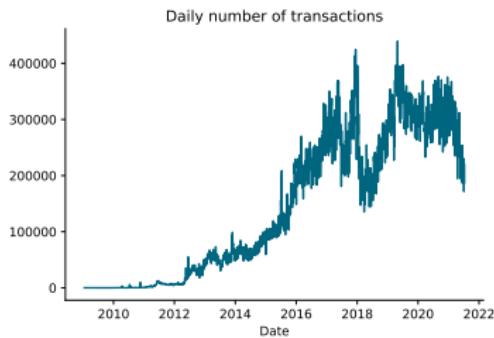
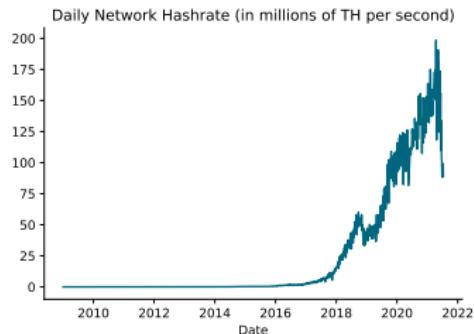
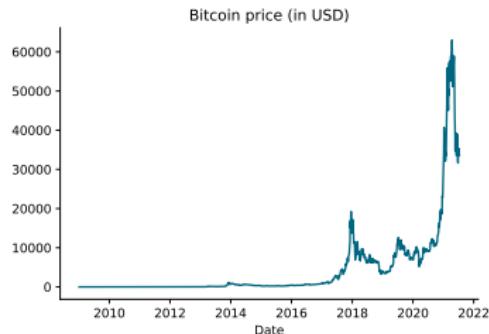
Blockchain parameters

- Consensus protocol (PoW or PoS)
 - ↳ Hash function (SHA-256 for Bitcoin and scrypt for LiteCoin)
 - ↳ Hybrid PoW/PoS (PeerCoin)
- Block generation time
 - ↳ every 10 minutes for Bitcoin
 - ↳ every 12 sec for Ethereum
- Block finding reward
 - ↳ Halved every 210,000 blocks in Bitcoin. It started at 50 BTC, is now 6.25 BTC
<https://www.bitcoinblockhalf.com/>
- Total coin supply
 - ↳ 21,000,000 in total for Bitcoin
- Transaction fees
 - ↳ GAS in Ethereum

These choices lead to the creation of multiple cryptocurrencies

Examples

Bitcoin and AltCoins (Ethereum, LiteCoin, DogeCoin, Ripple...), see https://en.wikipedia.org/wiki/List_of_cryptocurrencies



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
- + Permissionless
- + 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.

Tokenized real-world assets

Tokenized version of a real-world, physical asset

- Increases the liquidity of certain type of assets
- Make certain classes of assets available to the many
- Can be used as store of value or collateral

These token can be backed by

- fiat currency ⇒ stablecoin
- commodities like gold <https://ekon.gold/>
- stocks (security token) that includes voting right and profit sharing mechanism
- Art
- Digital art (Non Fungible tokens on the Ethereum blockchain)

Central authority

This requires a custodian to ensure that the tokens are actually backed by these off-chain assets (except for NFTs).



OECD, "The tokenisation of assets and potential implications for financial markets," tech. rep., 2020.

Valuation models

- Cryptocurrencies are medium of exchange and may be priced via transaction cost model (Beaumol-Tobin and such)
 - ❑ W. J. Baumol, "The transactions demand for cash : An inventory theoretic approach," *The Quarterly Journal of Economics*, vol. 66, p. 545, nov 1952.
 - ❑ L. Schilling and H. Uhlig, "Some simple bitcoin economics," *Journal of Monetary Economics*, vol. 106, pp. 16–26, oct 2019.
- Tokenized asset depends on the real asset that backs the token
 - ❑ J. Hargrave, N. Sahdev, and O. Feldmeier, "How value is created in tokenized assets," in *Blockchain Economics : Implications of Distributed Ledgers*, pp. 125–143, WORLD SCIENTIFIC (EUROPE), jan 2019.
- Utility tokens
 - ❑ J. R. Gan, G. Tsoukalas, and S. Netessine, "Initial coin offerings, speculation, and asset tokenization," *Management Science*, vol. 67, pp. 914–931, feb 2021.
 - ❑ L. W. Cong, Y. Li, and N. Wang, "Tokenomics : Dynamic adoption and valuation," *The Review of Financial Studies*, vol. 34, pp. 1105–1155, aug 2020.

ICO tuning and timeline

1 ICO period

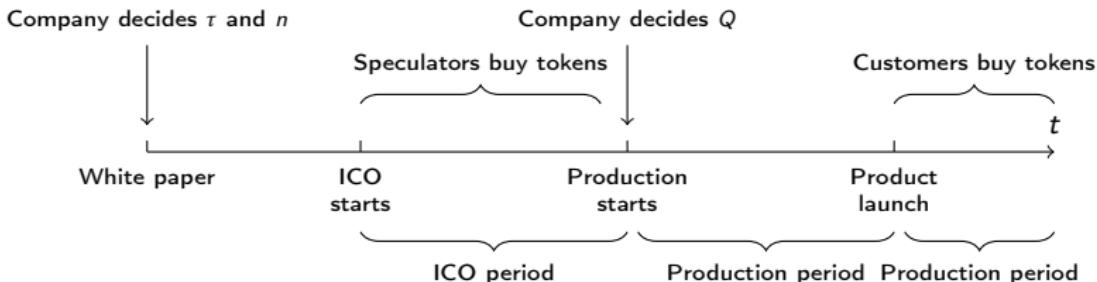
- The firm publishes a white paper and set
 - The token price τ
 - The total number of token m
 - The number of token issued to the investors during the ICO $n \leq m$.
- s among $z >> m$ investors buy token

2 Production period

- The firm uses the funds raised $s\tau$ to finance the production of Q units of goods

3 Market period

- Customers purchase token to meet their needs $D \sim F(\cdot)$



J. R. Gan, G. Tsoukalas, and S. Netessine, "Initial coin offerings, speculation, and asset tokenization," *Management Science*, vol. 67, pp. 914–931, feb 2021.

Insights

Optimal number of tokens sold n^*

The more token the firm sells during the ICO

- The more money to invest in production
- The less tokens it has to sell in the secondary market
- The less "skin in the game"
- The less it wants to invest in production ex post

n^* resolves the trade off between money now and money later while controlling moral hazard.

Optimal token price τ^*

- Price too low : Not enough funds raised
- Price too high : not enough upside for investors

Gerry Tsoukalas talk at

https://www.youtube.com/watch?v=E_NT4t4ws8U

Decentralized insurance

Parametric insurance

Compensation if a measurable quantity reaches a threshold

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