Stochastic Models for blockchain analysis

Introduction

Pierre-O. Goffard

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

9 juillet 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

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)

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

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

SHA-256

Applications of blockchain : Cryptocurrency

Bitcoin

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

Decentralized finance

Consensus protocols

The three dimension of blockchain systems analysis

1. Efficiency
2. Decentralization
3. Security

Proof of Work

Proof of Stake


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