# BLOCKASTICS

## Stochastic models for blockchain analysis

Pierre-O Goffard

March 18, 2022

# Chapter 1

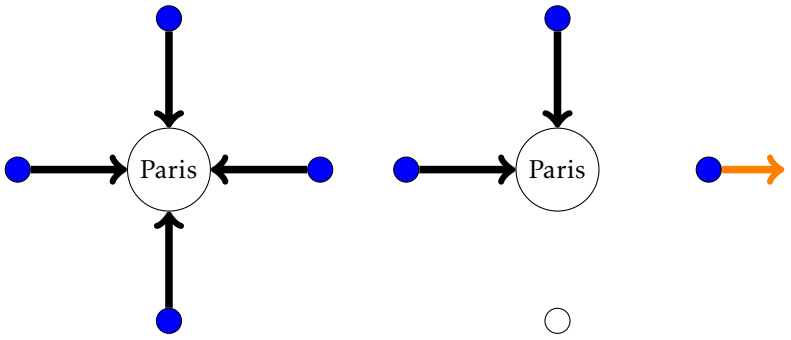
# Introduction

A blockchain is a distributed ledger maintained by achieving consensus among a number of nodes in a Peer-to-Peer network. The blockchain technology has attracted a lot of interest after the advent of the bitcoin cryptocurrency in 2008, see Nakamoto [2008]. Since then, the blockchain concept has been used to develop decentralized systems to store and maintain the integrity of time-stamped transaction data across peer-to-peer networks. Besides the creation of a digital currency, blockchain applications include the sharing of IT resources, the registration of authentication certificate or the implementation of smart contracts.

The topic of blockchain is of primary interest to computer scientists working on peer-to-peer networks and distributed algorithm. The problem of reaching consensus inside peer-to-peer networks is a classical problem framed as "The Byzantine general problem" by Lamport et al. [1982]. A group of generals from the Byzantine army is surrounding an enemy city. Communicating only by messenger, they must agree on a common battle plan. There may be traitors who will attack instead of retreat or non responding generals who will do nothing. For the project to be successful a majority of the general must either retreat or attack. The problem then reduces to finding an algorithm to ensure that the loyal generals reach an agreement. The problem is illustrated on Figure 1.1.

In a blockchain system, we have a large network of nodes that broadcast transactions which corresponds to pieces of information that will be written in the blockchain. light nodes, full nodes consensus and write information.

- Computer science
- Economics
- Applied math and operations research




(a) Coordinated attack

(b) Failed attack due to one traitor and one non-responding general

Figure 1.1: Illustration of the BYzantine general problem

# Chapter 2

# Consensus protocol

The problem of reaching consensus within a Peer-to-peer network is a very old problem in computer science. An obvious solution is to rely on a majority vote. This is the solution proposed by SHostak and his co-author who, in passing, make a famous analogy with Byzantine generals trying to agree on a common battle plan. Here the battle plan corresponds to adding a new block with a set of transactions deemed valid and therefore agreeing on a common data history. A voting system inside a large network involves a colossal number of messages exchanged leading to the consumption of all the bandwidth, the failure of certain nodes by denial of service and delays in the synchronization of the network. Castro and Liskov's Practical Byzantine Fault Tolerance (PBFT) algorithm is the gold standard for practical implementation of a voting system within a peer-to-peer network. Despite these recent advances, such a system is not suitable for a network that can grow indefinitely. Bitcoin solved this scaling problem by proposing a system based on the election of a leader making unilateral decisions. The Proof of Work protocol appoints a leader based on its computing resources. Each node competes to solve a puzzle with a brute force search algorithm. The first node who is able to propose a solution append the next block. The search for a solution, referred to as mining, is associated with an operational cost borne by the nodes which is compensated by a reward expressed in the native blockchain cryptocurrency. The surge in cryptocurrency prices has led to a rush in block mining, leading to a major spike in the electricity consumption and electronic waste generation of blockchain networks. The blockchain network consumes as much electricity as countries the size of Thailand at the time of the writing. The need for a more restricted consensus protocol therefore becomes crucial. These remain based on the election of a leader but rely on other network resources. The Proof-of-Stake protocol sample the nodes with The proof of storage (no arm race, no electronic waste and useful like the file coin project)

## 2.1 Voting system

## 2.2 Leader system

- Public blockchain,
- operational cost,
- reward,
- incentive compatible
- Uses the scarce ressource of the network
  - Computational power (CPU, GPU)
  - Bandwidth
  - Storage space
  - Crypto coins

### 2.2.1 Proof-of-Work

### 2.2.2 Proof-of-Stake

# Chapter 3

# Security of blockchain systems

## 3.1 Double-spending in PoW

### 3.1.1 Random walk model

#### Double spending probability

#### Double spending time

### 3.1.2 Counting process model

#### Double spending probability

#### Double spending time

## 3.2 Blockwitholding in PoW

## 3.3 Nothing-at-stake in PoS

# Chapter 4

# Decentralization of blockchain system

## 4.1 Decentralization in PoS

Rich get richer? Polya's urn

### 4.1.1 Average stake own by each peer

### 4.1.2 Distribution of the stakes

## 4.2 Decentralization in PoW

### 4.2.1 Mining pools and reward systems

### 4.2.2 Mining pool risk analysis

# Chapter 5

# Efficiency of blockchain systems

## 5.1 A queueing model with bulk service

## 5.2 Latency and throughputs computation

# Bibliography

Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, pages 382–401, July 1982. URL https://www.microsoft.com/en-us/research/publication/byzantine-generals-problem/.

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