

# unsw

Sydney



# unsw

Sydney



UNSSW Sydney

# Blockchain and applications

Pierre-O. Goffard

Université de Strasbourg  
[goffard@unistra.fr](mailto:goffard@unistra.fr)

27 octobre 2023

# Agenda

- 1 Introduction
- 2 Consensus protocol
- 3 Cryptocurrencies and Decentralized Finance (and insurance)

# Agenda

## Introduction

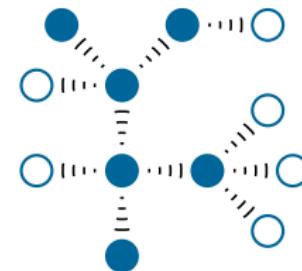
- 1 Introduction
- 2 Consensus protocol
- 3 Cryptocurrencies and Decentralized Finance (and insurance)

# Blockchain

## Introduction

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



# Consensus protocols

## Introduction

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

# Applications of blockchain : Cryptocurrency

## Introduction

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



- Transaction anonymity
- No need for a trusted third party

# Agenda

## Consensus protocol

1 Introduction

2 Consensus protocol

3 Cryptocurrencies and Decentralized Finance (and insurance)

# Consensus protocol

## Consensus protocol

### Definition

Algorithm to allows the full nodes to agree on a common data history

It must rely on the scarce resources of the network

- bandwidth
- computational power
- storage (disk space)

# Types of consensus protocols

## Consensus protocol

### 1 Voting based

 L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Transactions on Programming Languages and Systems*, pp. 382–401, July 1982.

-  Communication overhead
-  Denial of service

### 2 Leader based

- Proof-of-Work (computational power)
- Proof-of-Capacity and Proof-of-Spacetime (storage)
- Proof-of-Interaction (bandwidth)
- Proof-of-Stake (tokens)

# Proof-of-Work

Consensus protocol

## Objective

Elect a leader based on computational effort to append the next block.

# What's inside a block ?

Consensus protocol

A block consists of

- a header
- a list of "transactions" that represents the information recorded through the blockchain.

The header usually includes

- the date and time of creation of the block,
- the block height which is the index inside the blockchain,
- the hash of the block
- the hash of the previous block.

Question

What is the hash of a block ?

# Cryptographic Hash function

## Consensus protocol

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

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

# SHA-256

Consensus protocol

The SHA-256 function which converts any message into a hash value of 256 bits.

## Example

The hexadecimal digest of the message

Is DeFi the future?

is

60a147c28568dc925c347bce20c910ef90f3774e2501ac63344f3411b6a6bf79

# Hidden prediction

Consensus protocol



**Matt Levine** @matt\_levine

Here is a SHA-256 hash of a prediction I am making:

64b70b0494580b278d7f1f551d482a3fb952a4b018b43090ffeb87b662d34847.



M. Levine, "The crypto story." Bloomberg business week, Oct. 2022.

# Mining a block

## Consensus protocol

```
Block Hash: 1fc23a429aa5aaf04d17e9057e03371f59ac8823b1441798940837fa2e318aaa
Block Height: 0
Time:2022-02-25 12:42:04.560217
Nonce:0
Block data: [{"sender": "Coinbase", "recipient": "Satoshi", "amount": 100, "fee": 0}, {"sender": "Satoshi", "recipient": "Pierre-O", "amount": 5, "fee": 2}]
Previous block hash: 0
Mined: False
-----
```

Figure – A block that has not been mined yet.

# Mining a block

Consensus protocol

The maximum value for a 256 bits number is

$$T_{\max} = 2^{256} - 1 \approx 1.16e^{77}.$$

Mining consists in drawing at random a nonce

$$\text{Nonce} \sim \text{Unif}(\{0, \dots, 2^{32} - 1\}),$$

until

$$h(\text{Nonce} | \text{Block info}) < T,$$

where  $T$  is referred to as the target.

Difficulty of the cryptopuzzle

$$D = \frac{T_{\max}}{T}.$$

<https://laub.au/mine/>

# Mining a block

## Consensus protocol

If we set the difficulty to  $D = 2^4$  then the hexadecimal digest must start with at least 1 leading 0

```
Block Hash: 0869032ad6b3e5b86a53f9dded5f7b09ab93b24cd5a79c1d8c81b0b3e748d226
Block Height: 0
Time:2022-02-25 13:41:48.039980
Nonce:2931734429
Block data: [{"sender": "Coinbase", "recipient": "Satoshi", "amount": 100, "fee": 0}, {"sender": "Satoshi", "recipient": "Pierre-O", "amount": 5, "fee": 2}]
Previous block hash: 0
Mined: True
-----
```

Figure – A mined block with a hash value having one leading zero.

The number of trials is geometrically distributed

- Exponential inter-block times
- Length of the blockchain = Poisson process

# Conflict resolution in blockchain

## Consensus protocol

### Fork

A fork arises when there is a disagreement between the nodes resulting in several branches in the blockchain.

### LCR

The *Longest Chain Rule* states that if there exist several branches of the blockchain then the longest should be trusted.

## In practice

- A branch can be considered legitimate if it is  $k \in \mathbb{N}$  blocks ahead of its pursuers.
- Fork can be avoided when

block appending time > propagation delay

# Bitcoin protocol

## Consensus protocol

- One block every 10 minutes on average
- Depends on the hashrate of the network
- Difficulty adjustment every 2,016 blocks ( $\approx$  two weeks)
- Reward halving every 210,000 blocks

---

. <https://www.bitcoinblockhalf.com/>

# Mining equipments

## Consensus protocol

How it started

- CPU, GPU

How it is going

- Application Specific Integrated Chip (ASIC)
  - Network electricity consumption
  - E-Waste
  - Centralization issue

# Proof of Stake

Consensus protocol

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

PoS

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

Nodes are chosen according to what they own.

- Nothing at stake problem
- Rich gets richer ?
- <https://www.peercoin.net/>



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

# Agenda

Cryptocurrencies and Decentralized Finance (and insurance)

- 1 Introduction
- 2 Consensus protocol
- 3 Cryptocurrencies and Decentralized Finance (and insurance)

# TradFi Pain Points I

Cryptocurrencies and Decentralized Finance (and insurance)

## 1 Access barrier

- TradFi Criteria ⇒ bank account
- DeFi No Barrier

## 2 Centralization

- TradFi Bank are record keepers ⇒ Cyber risk
- DeFi Decentralized Ledger

## 3 High costs and intermediation

- TradFi Transaction fees, account maintenance fees, wire transfer fees,...
- DeFi Intermediaries ⇒ Smart contracts (Gas fees)

## 4 Slow transaction settlement

- TradFi Cross border transactions ⇒ Takes day to be settled
- DeFi Near instant settlement (30 min on the bitcoin blockchain)

## 5 Transparency and auditability

- TradFi Difficulty to verify the accuracy of transactions and asset holding
- DeFi Publicly available ledger and open source code

# TradFi Pain Points II

Cryptocurrencies and Decentralized Finance (and insurance)

## 6 Censorship and restrictions

- TradFi Asset in custody, censorship by governments
- DeFi No interference of central authority

## 7 Global accessibility

- TradFi Respect the operating hours
- DeFi Operates 24/7

## 8 Fractional ownership

- TradFi Real estate and art work are not divisible
- DeFi Tokenized real world assets

## 9 Innovation and interoperability

- TradFi Use outdated IT solutions
- DeFi Interoperability between platforms and project



A. Lipton and A. Treccani, *Blockchain and Distributed Ledgers*.  
WORLD SCIENTIFIC, apr 2021.

# Cryptocurrencies

## Cryptocurrencies and Decentralized Finance (and insurance)

- 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

Cryptocurrencies and Decentralized Finance (and insurance)

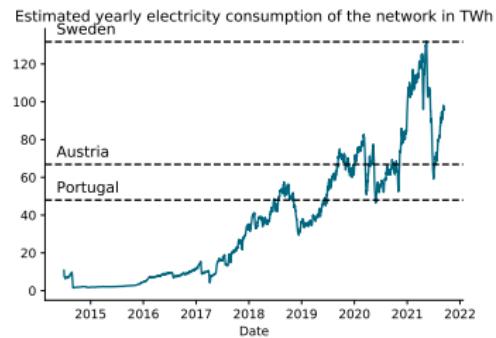
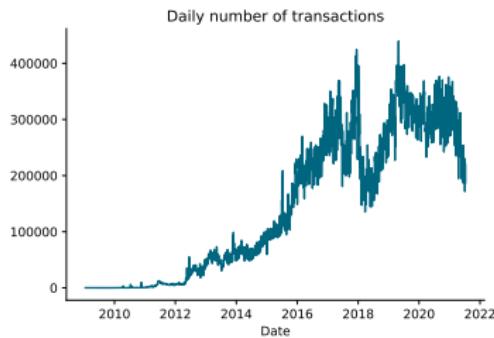
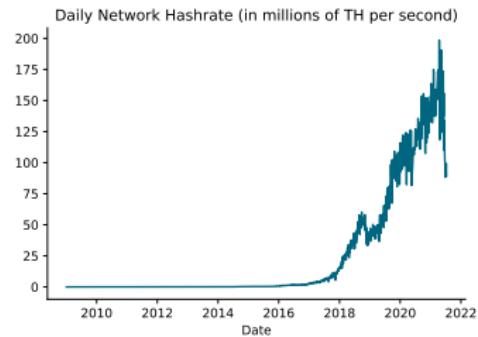
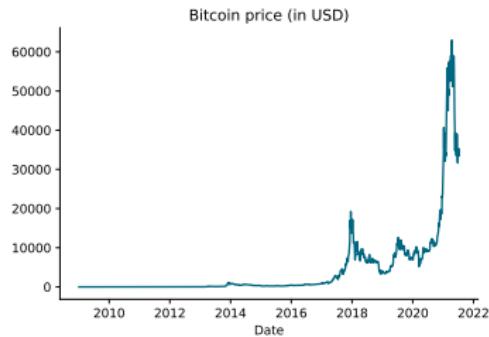
Blockchain parameters

- Consensus protocol (PoW or PoS)
  - ↳ Hash function (SHA-256 for Bitcoin and scrypt for LiteCoin)
  - ↳ Hybrid PoW/PoS (PeerCoin)
- Block generation time (<https://txstreet.com/v/eth-btc>)
  - ↳ 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](https://en.wikipedia.org/wiki/List_of_cryptocurrencies)



# Decentralized finance

Cryptocurrencies and Decentralized Finance (and insurance)

DeFi extends the Bitcoin promises to more complex financial operations

- Collateralized lending
- Decentralized Exchange Platform
- Tokenized assets

Thanks to Smart Contract on the Ethereum blockchain.



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

---

. <https://uniswap.org/>

# Decentralized Exchange platforms

Cryptocurrencies and Decentralized Finance (and insurance)

## Centralized Exchange

Binance, Coinbase, Kraken,...

⇒ Order book

## Decentralized Exchange

Exchange where you trade one token for another through a smart contract on the Ethereum blockchain (ETH).

⇒ Automated Market Makers (AMM) and Liquidity Providers (LPs)

# Order book

Cryptocurrencies and Decentralized Finance (and insurance)

Table – Buy Orders

Price	Quantity	Total
9,950	10	99,500
9,900	5	49,500

Table – Sell Orders

Price	Quantity	Total
10,100	2	20,200
10,200	15	153,000

and a market maker in the middle to offer liquidity...

⚠ Lots of transaction must be issued

- Slow (10-15 txs/s)
- Expensive (gas fees)

# Order book

Cryptocurrencies and Decentralized Finance (and insurance)

Table – Buy Orders

Price	Quantity	Total
9,950	10	99,500
9,900	5	49,500

Table – Sell Orders

Price	Quantity	Total
10,100	2	20,200
10,200	15	153,000

and a market maker in the middle to offer liquidity...

⚠ Lots of transaction must be issued

- Slow (10-15 txs/s)
- Expensive (gas fees)

# Automated Market Makers (AMM)

Cryptocurrencies and Decentralized Finance (and insurance)

A blockchain requires an algorithm  $\Rightarrow$  AMM

- Exchange one token against another, usually Crypto/Stable Coins
- Constant Function Market Makers
- Liquidity Providers



## Stable Coin

A bridge from fiat to crypto currency

- Fiat-Collateralized Stablecoins (e.g. USDC backed by one USD)
- Crypto-Collateralized Stablecoins (e.g. DAI backed by crypto locked in a smart contract)

# Constant Product Market Maker

Cryptocurrencies and Decentralized Finance (and insurance)

Let  $k$  be a constant such that

$$x \cdot y = k,$$

- $x$  is the amount of token  $X$
- $y$  is the amount of token  $Y$

## Example

ETH/DAI even Constant Product Market Maker

- Say that the price for one ETH is  $P = \$500$
- A first LP provides 20 ETH plus 10,000 DAI which sets

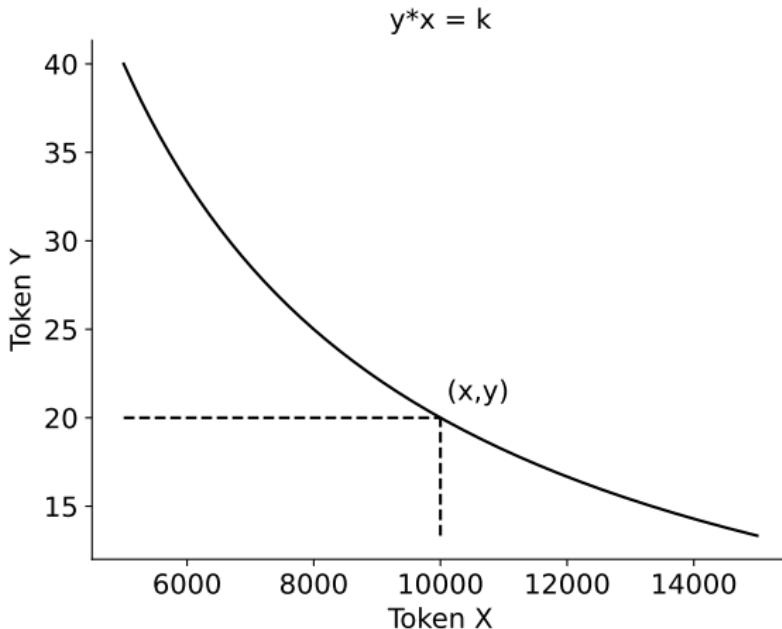
$$k = 20,000$$

- The liquidity provided is measured by

$$L = \sqrt{x \cdot y} \approx 447 \text{ (geometric mean)}$$

# Trade on a curve

Cryptocurrencies and Decentralized Finance (and insurance)



- . The pool never runs out of  $X$  nor  $Y$

# Swap $X$ for $Y$

Cryptocurrencies and Decentralized Finance (and insurance)

Acquire  $dy$  of token  $Y$ , then deposit  $dx$  that solves

$$(x + dx)(y - dy) = k \Leftrightarrow dx = \frac{x \cdot dy}{y - dy}$$

and pay a fee  $\alpha \cdot dx$  to the LPs.

⇒ Price of  $Y$  rise in the pool

## Example

Arbitrageur takes 2 ETH then deposits

$$dx = 1,111$$

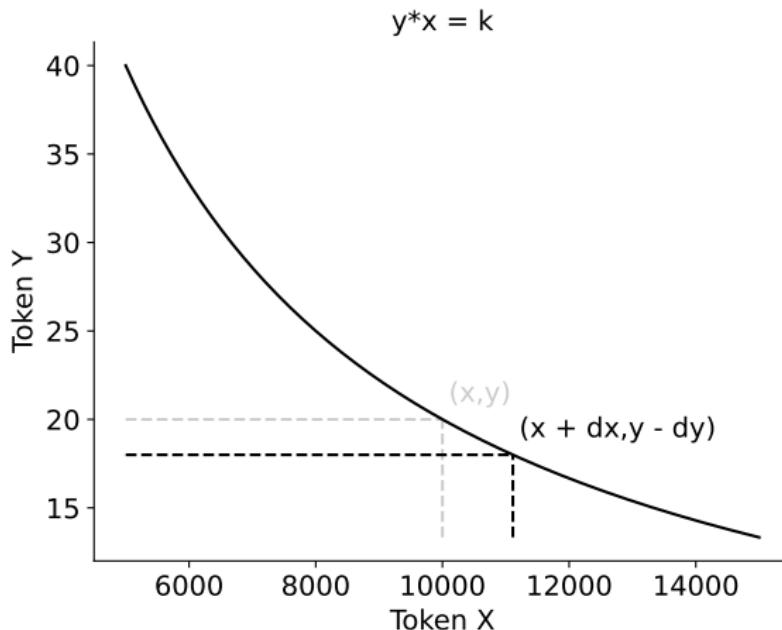
and give out  $0.3 \cdot 1,111 = 333$  worth of fees

- The price of ETH in the pool rises to

$$\frac{x + dx}{y - dy} = \$617.$$

# Trade on a curve

Cryptocurrencies and Decentralized Finance (and insurance)



# Add Liquidity

Cryptocurrencies and Decentralized Finance (and insurance)

Another LP provides  $dx$  of token  $X$  and thus  $dy = \frac{y}{x} dx$  (the price must not change)

- New level  $k' = (x + dx)(y + dy)$
- Liquidity rises  $L' = \sqrt{x \cdot y} + \sqrt{dx \cdot dy}$
- LPs are weighted according to the liquidity they provide
- Fees are distributed according to these weights

## Example

New LP deposits \$5,000 worth of tokens to the pool then

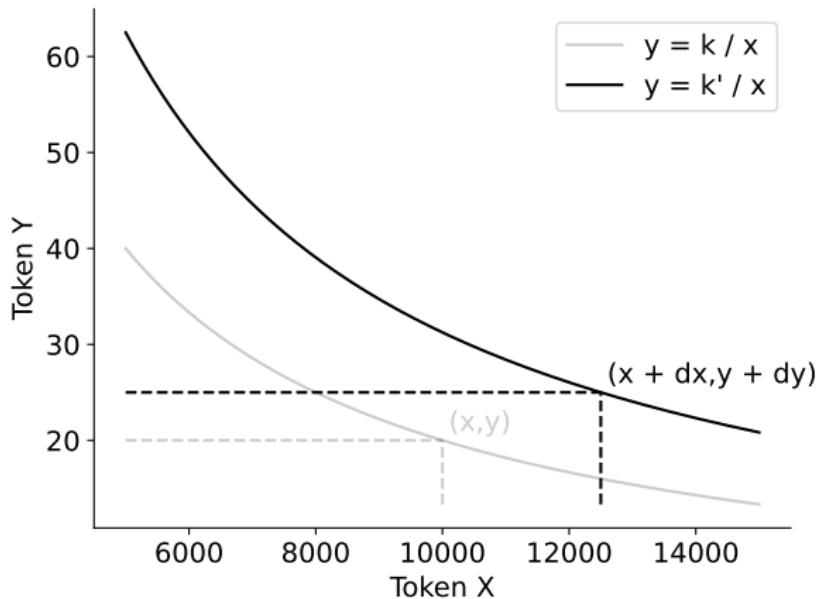
- $dx = 2,500$
- $dy = 5$
- $k' = 312,500$
- $L' \approx 559$

The weights are

$$\frac{L}{L'} = 0.8 \text{ and } \frac{L' - L}{L'} = 0.2.$$

# Trade on a new curve

Cryptocurrencies and Decentralized Finance (and insurance)



# Impermanent Loss

Cryptocurrencies and Decentralized Finance (and insurance)

Holding tokens VS Locking Tokens in a Smart Contract

# Impermanent Loss

Cryptocurrencies and Decentralized Finance (and insurance)

The price of  $Y$  in the pool is given by

$$P = \frac{x}{y},$$

in terms of token  $X$ .

- Price of  $Y$  becomes  $P' > P$  on another trading venue then arbitrageurs wish to find

$$\underset{dy > 0}{\operatorname{argmax}} dy \cdot P' - dx \cdot (1 + \alpha) = \underset{dy}{\operatorname{argmax}} dy \cdot P' - \frac{x \cdot dy}{y - dy} (1 + \alpha)$$

- We have

$$dy^* = y - \sqrt{\frac{k(1 + \alpha)}{P'}}$$

- The arbitrageurs profit is

$$dy^* \cdot P' - dx^* (1 + \alpha)$$

- It coincides with the impermanent loss of the LPs

$$y \cdot P' + x - [(y - dy^*) \cdot P' + x + dx^* (1 + \alpha)]$$

# Impermanent Loss

Cryptocurrencies and Decentralized Finance (and insurance)

The loss becomes permanent if

- The LPs withdraw their funds
- The price of the asset is not mean reverting

## Example

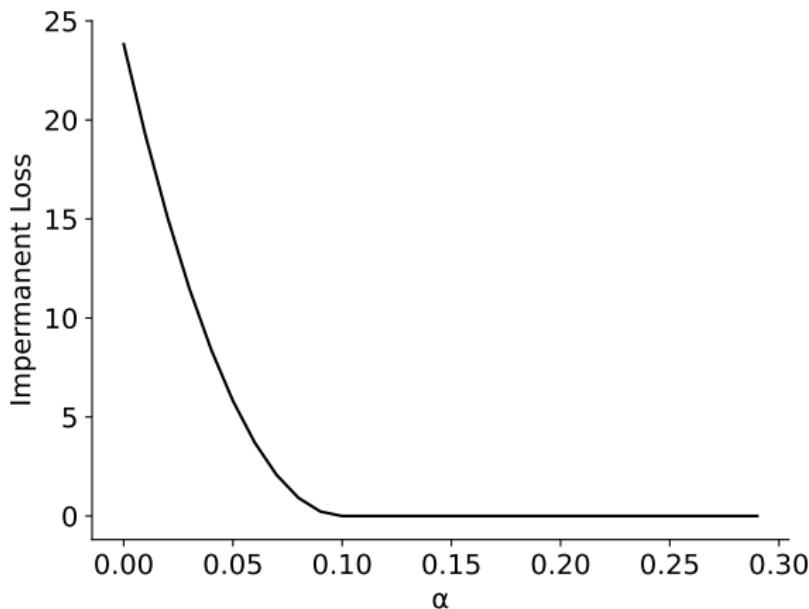
Suppose that  $P' = \$550$  and  $\alpha = 0$  then

- $dy^* = 0.93$
- The impermanent loss is then  $dy^* \cdot P' - \frac{xdy^*}{y-dy^*} = \$23$

# Impermanent loss

Cryptocurrencies and Decentralized Finance (and insurance)

The trading fee allows a pool to mitigate the impermanent loss



# Decentralized insurance

Cryptocurrencies and Decentralized Finance (and 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

# Blockchain as a research topic

Cryptocurrencies and Decentralized Finance (and insurance)

- Computer science
  - Peer-to-peer networks and consensus algorithm
  - Cryptography and security
- Economics
  - Game theory to study the incentive mechanism at play
  - Nature of the cryptoassets
- Operations research
  - Optimization of complex system
- Financial math
  - Valuation models for cryptoassets
- Machine learning and statistics
  - Open data
  - Interaction between blockchain users
  - (Social) network analysis
  - Clustering of public keys and addresses in the bitcoin blockchain.

# Byzantine General problem

$n$  generals must agree on a common battle plan, to either

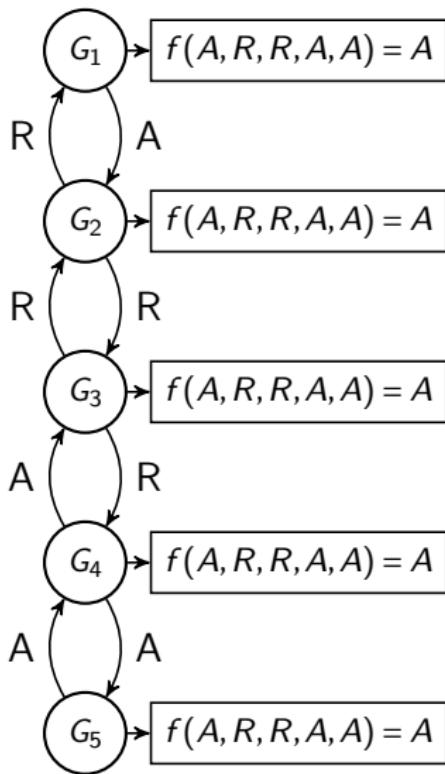
- Attack (A)
- Retreat (R)

## Problem

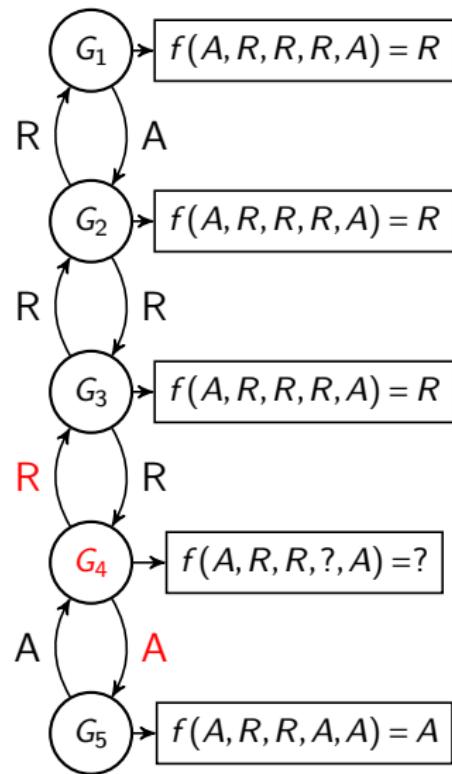
There are  $m < n$  traitors among the generals

- 1 message  $m(i,j)$  is sent to general  $j$  by general  $i$
- 2 Consensus is reached as general  $j$  applies

$$f(\{m(i,j); i = 1, \dots, n\}) = \begin{cases} A, & \text{if } \sum_{i=1}^n \mathbb{I}_{m(i,j)=A} > n/2, \\ R, & \text{else.} \end{cases}$$



(e) No traitor



(f) One traitor

Figure – Majority vote with or without a traitor

# Commanders and Lieutenants

One general is the commander while the others are the lieutenants

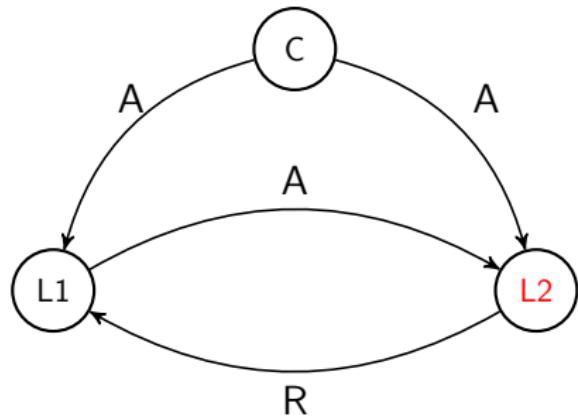
## Objective

Design an algorithm so that the following conditions are met :

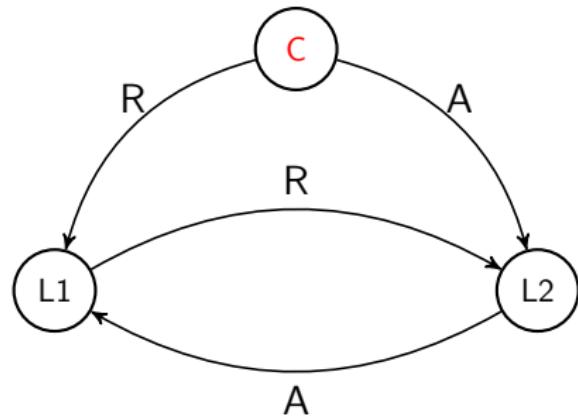
- C1 All the loyal lieutenants obey the same order
- C2 If the commanding general is loyal, then every loyal lieutenants obey the order he sends

## Byzantine Fault Tolerance Theorem (Lamport et al.)

There are no solution to the Byzantine General problem for  $n < 3m+1$  generals, where  $m$  is the number of traitors.



(a) Commander is loyal



(b) Commander is a traitor

Figure – Majority vote with or without a traitor

$n=4$  and  $m=1$  : Step 1

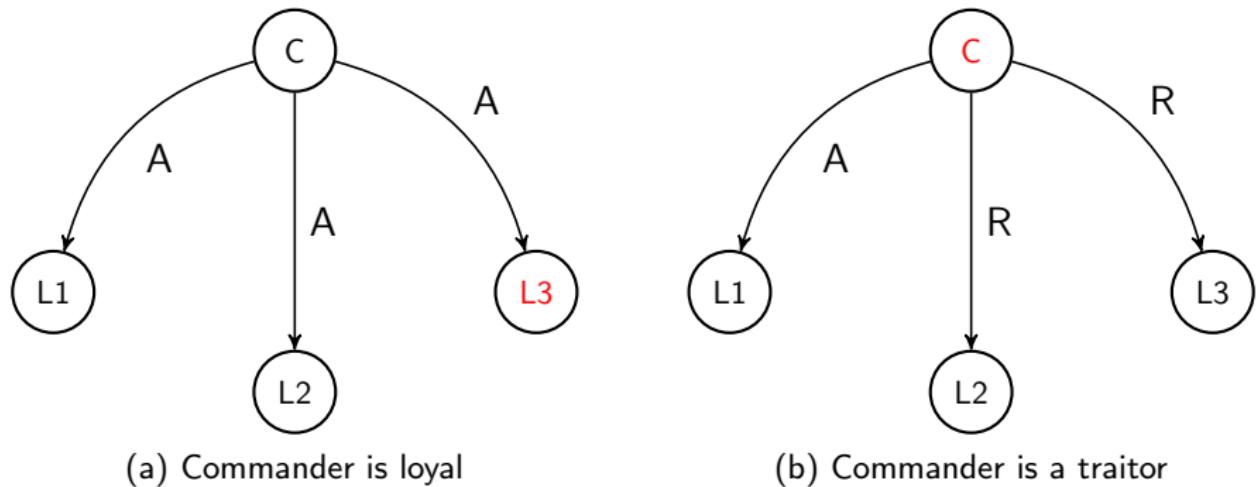
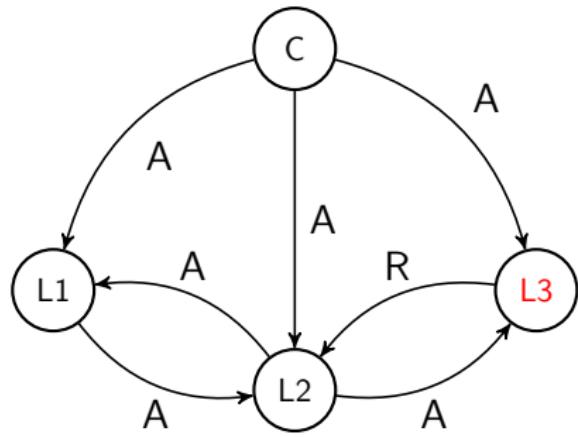
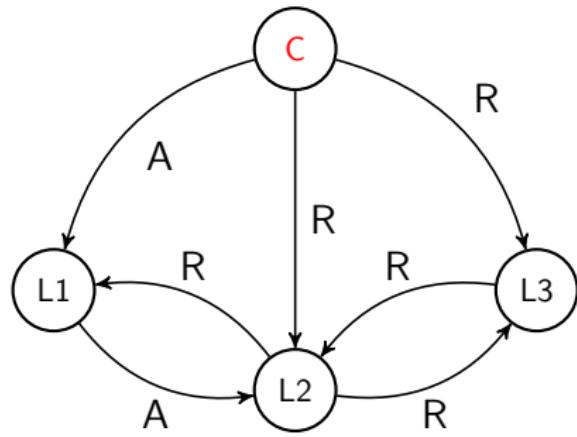


Figure – Illustration of the OM( $m$ ) algorithm in the case where  $n=4$  and  $m=1$ .

$n=4$  and  $m=1$  : Step 2



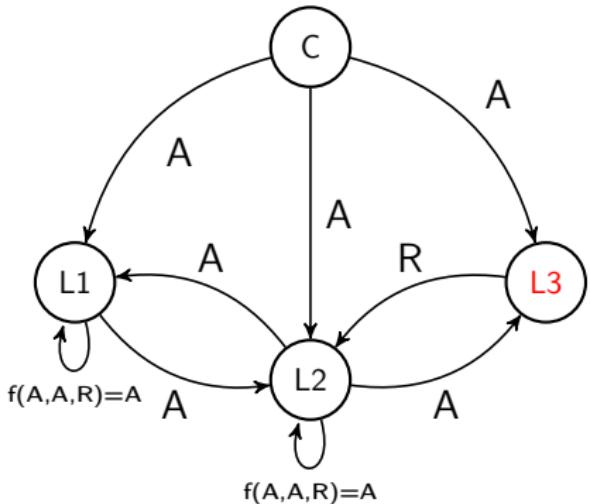
(a) Commander is loyal



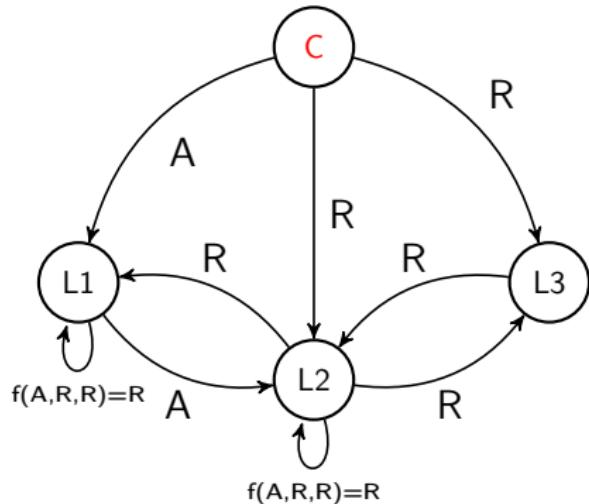
(b) Commander is a traitor

Figure – Illustration of the OM( $m$ ) algorithm in the case where  $n=4$  and  $m=1$ .

*n = 4* and *m = 1* : Step 3



(a) Commander is loyal,  $C_1$  and  $C_2$



(b) Commander is a traitor,  $C_1$

Figure – Illustration of the OM( $m$ ) algorithm in the case where  $n = 4$  and  $m = 1$ .

# The problem with majority vote

The OM algorithm requires to send  $n^{m+1}$

- ⚠ Communication overhead
- ⚠ Denial of service

## Solution

Leader based protocols !