Blockchain and Applications

Chapter 1

What is a blockchain ?

Clement Germanicus

CENTRALE PARIS

EPFL

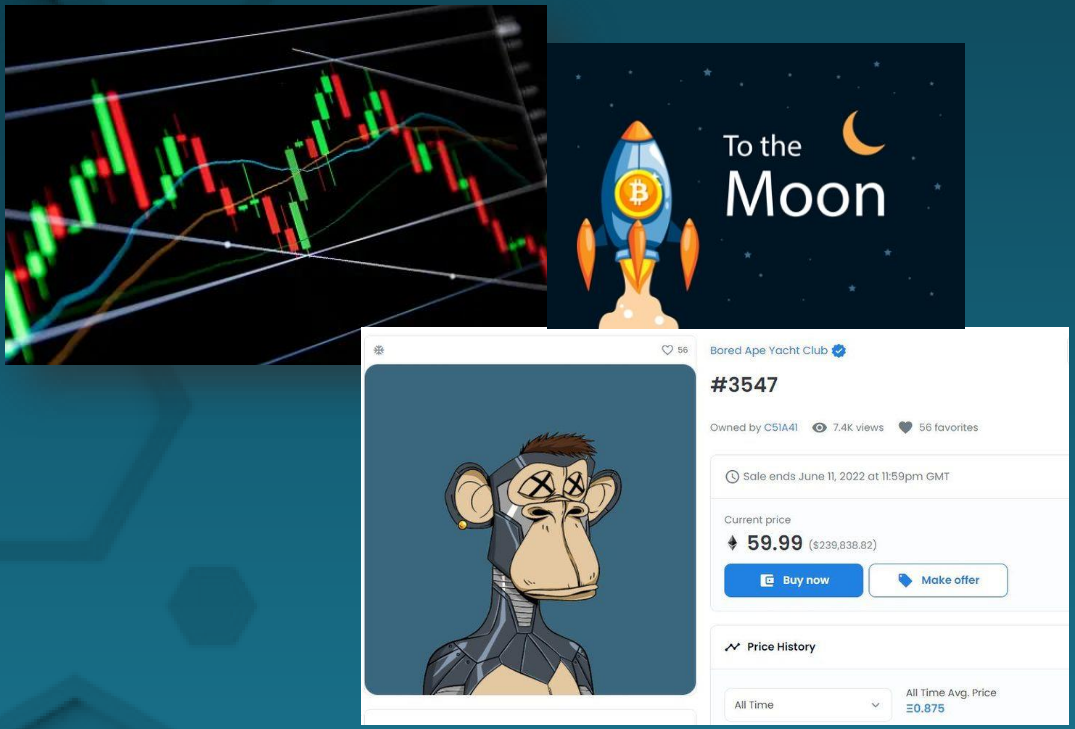
2017

Acid Cousins

Co-founder

2020

What you get/don't get in this module



Bored Ape Yacht Club

#3547

Owned by C51A41 7.4K views 56 favorites

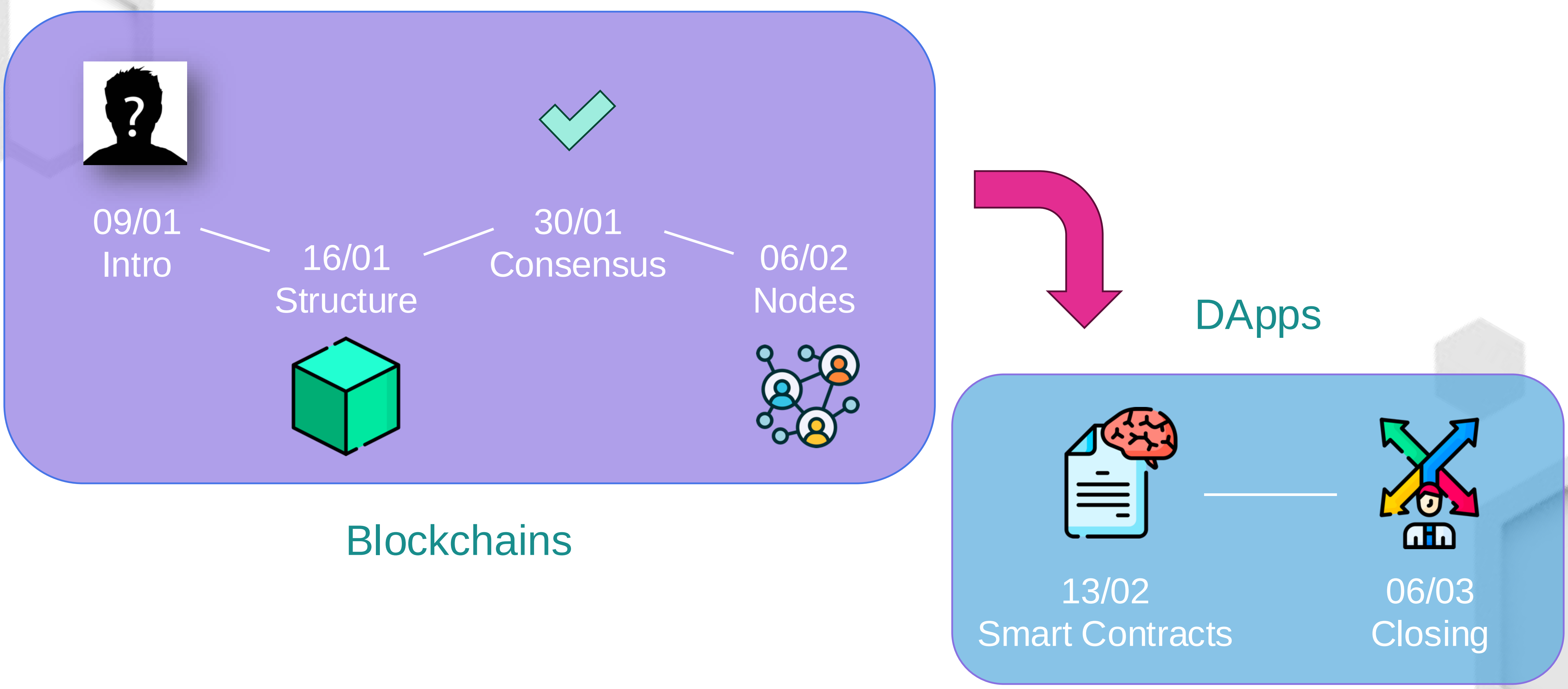
Sale ends June 11, 2022 at 11:59pm GMT

Current price

59.99 ($239,838.82)

All Time Avg. Price
Ξ0.875

Module schedule



09/01
Intro

16/01
Structure

30/01
Consensus

06/02
Nodes

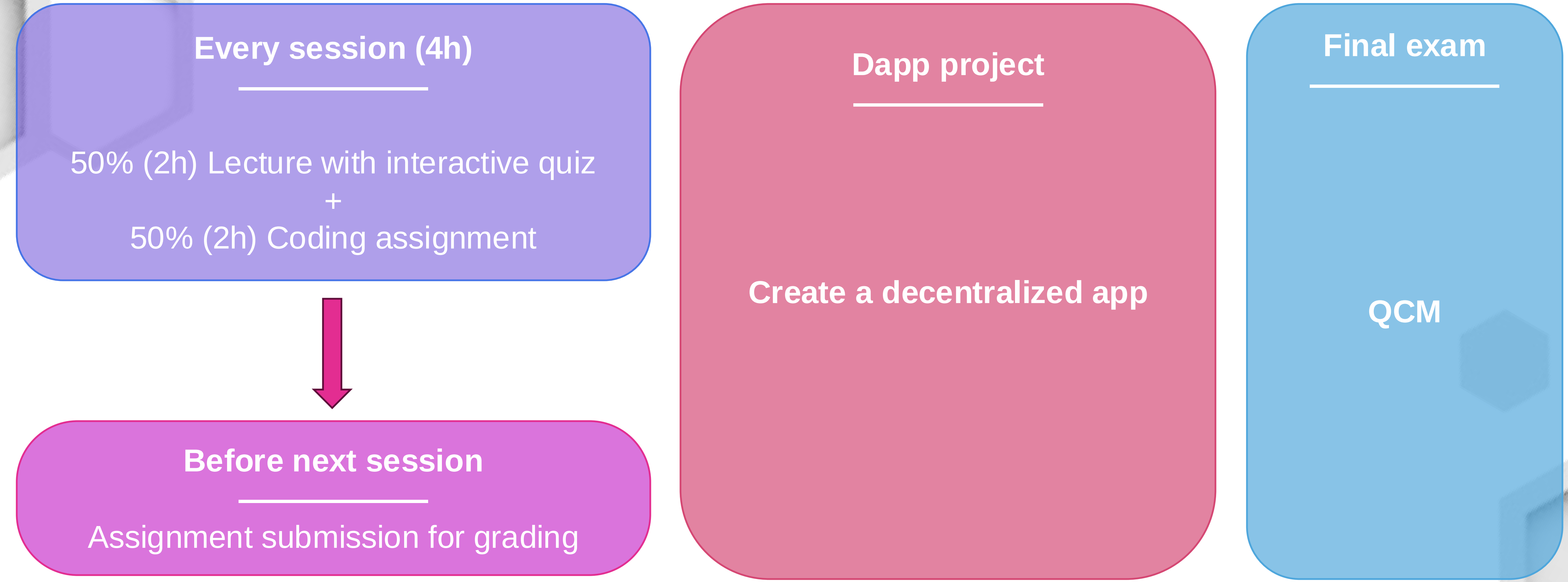
Blockchains

DApps

13/02
Smart Contracts

06/03
Closing

Session and evalutaion mechanisms



Every session (4h)

50% (2h) Lecture with interactive quiz
+
50% (2h) Coding assignment

Before next session

Assignment submission for grading

Dapp project

Create a decentralized app

Final exam

QCM

30% of final grade

20%

50%

Session and evalutaion mechanisms

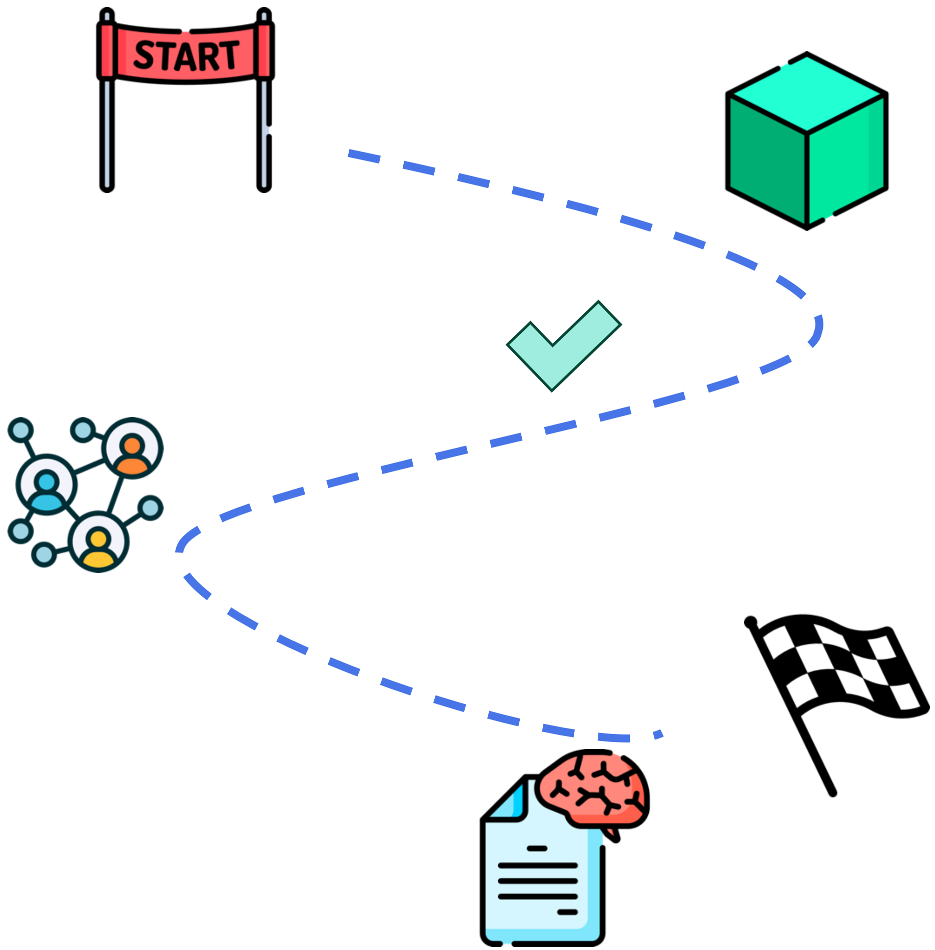
Every session (4h)

50% (2h) Lecture with interactive quiz
+
50% (2h) Coding assignment

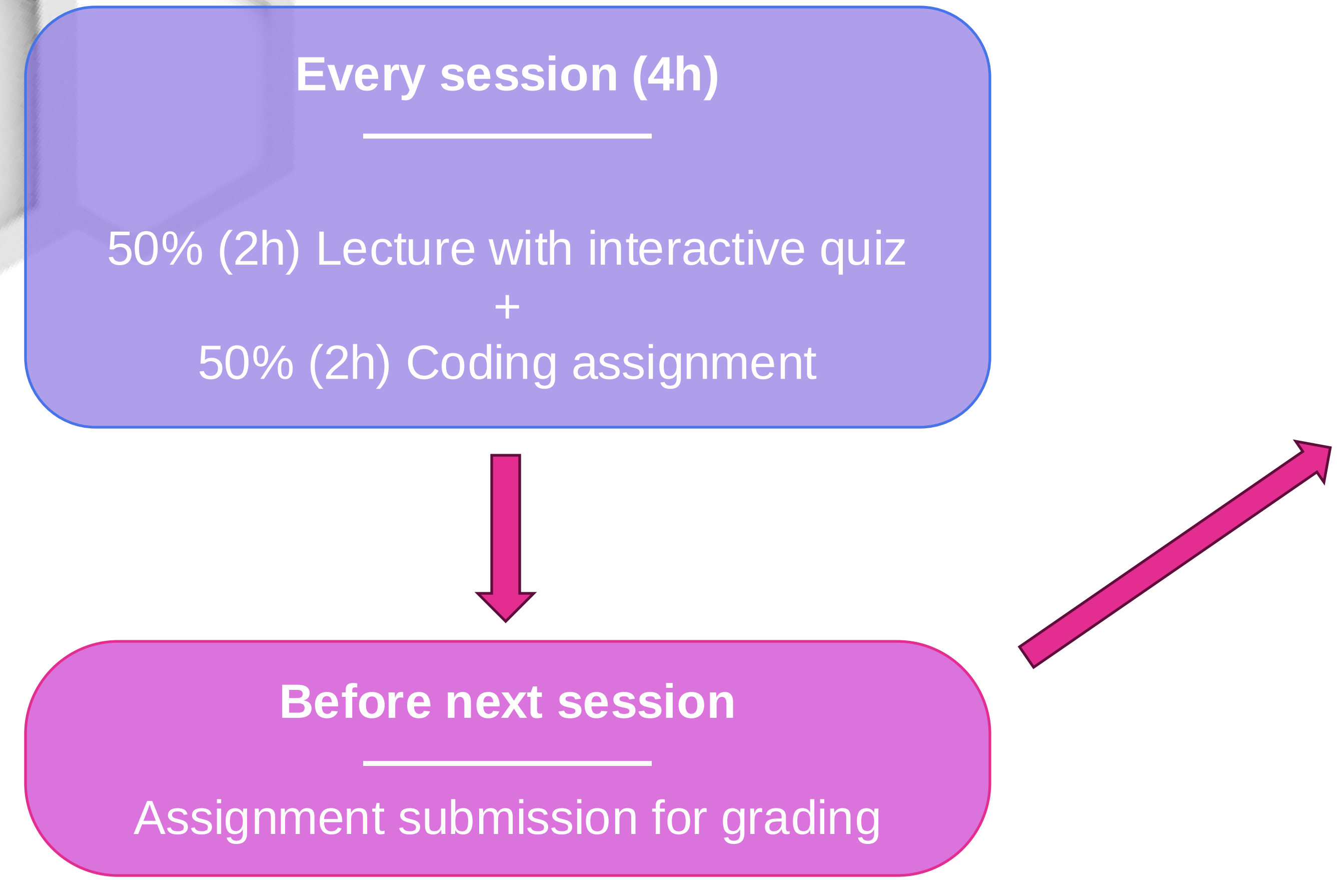
Before next session

Assignment submission for grading

30% of final grade



Session and evalutaion mechanisms



Every session (4h)

50% (2h) Lecture with interactive quiz
+
50% (2h) Coding assignment

Before next session

Assignment submission for grading

You will be graded using a hidden notebook

30% of final grade

Rules of this module

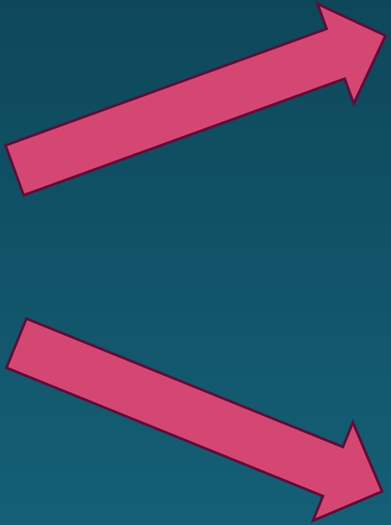
- Late arrivals
  - 5 min ok
  - After 5 min : you wait until the break (after 2h)

- Coding assignments
  - Python ONLY
  - Submit your whole “Assignments” folder as a zip
  - It’s ok to help others, but copying code will be granted a 0 : your code will be analyzed by an algorithm
  - ChatGPT is allowed but if I can detect it, you’ll get 0
  - Better give me an unfinished work than a cheated one

- Contact me!
  - By email : clement.germanicus@ext.junia.com
  - On Teams

When was blockchain born ?

David Chaum — 1982

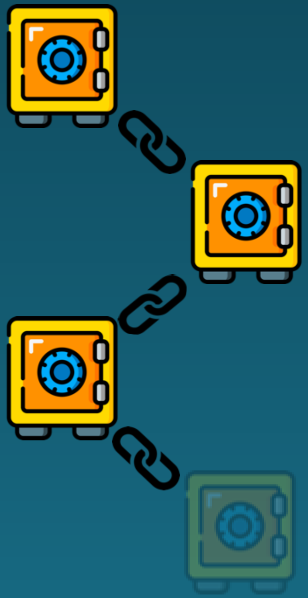


Electronic cash

Paying anonymously

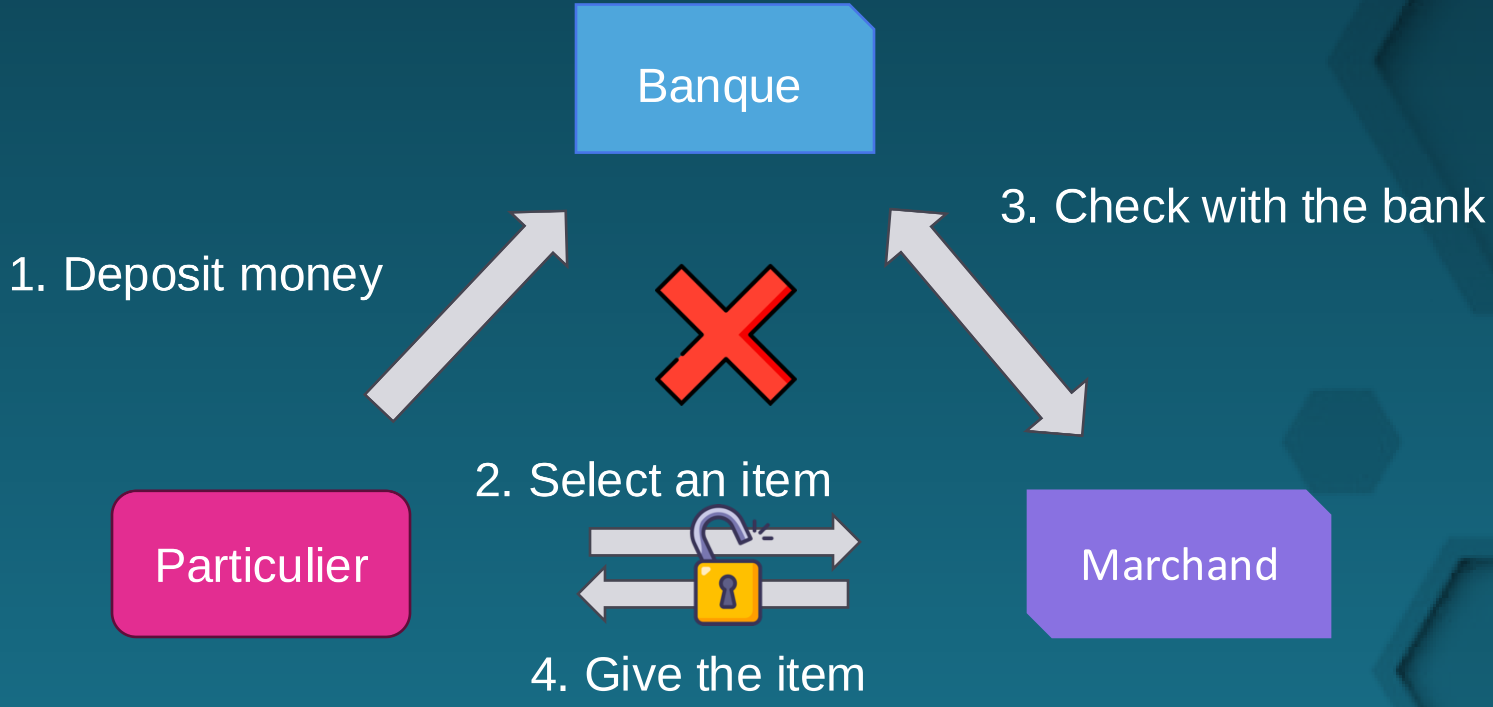
David Chaum — 1982

1982 — “Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups”

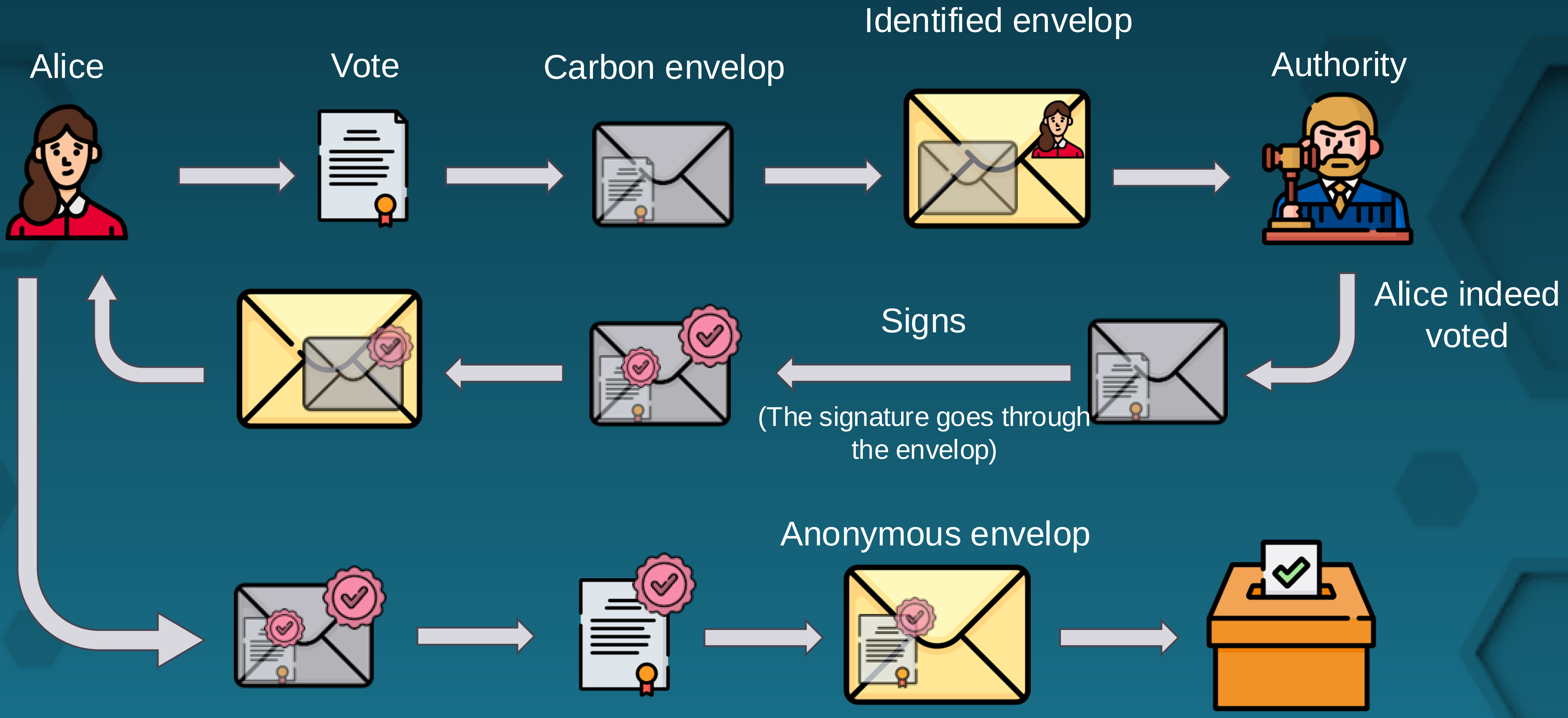


David Chaum — 1982

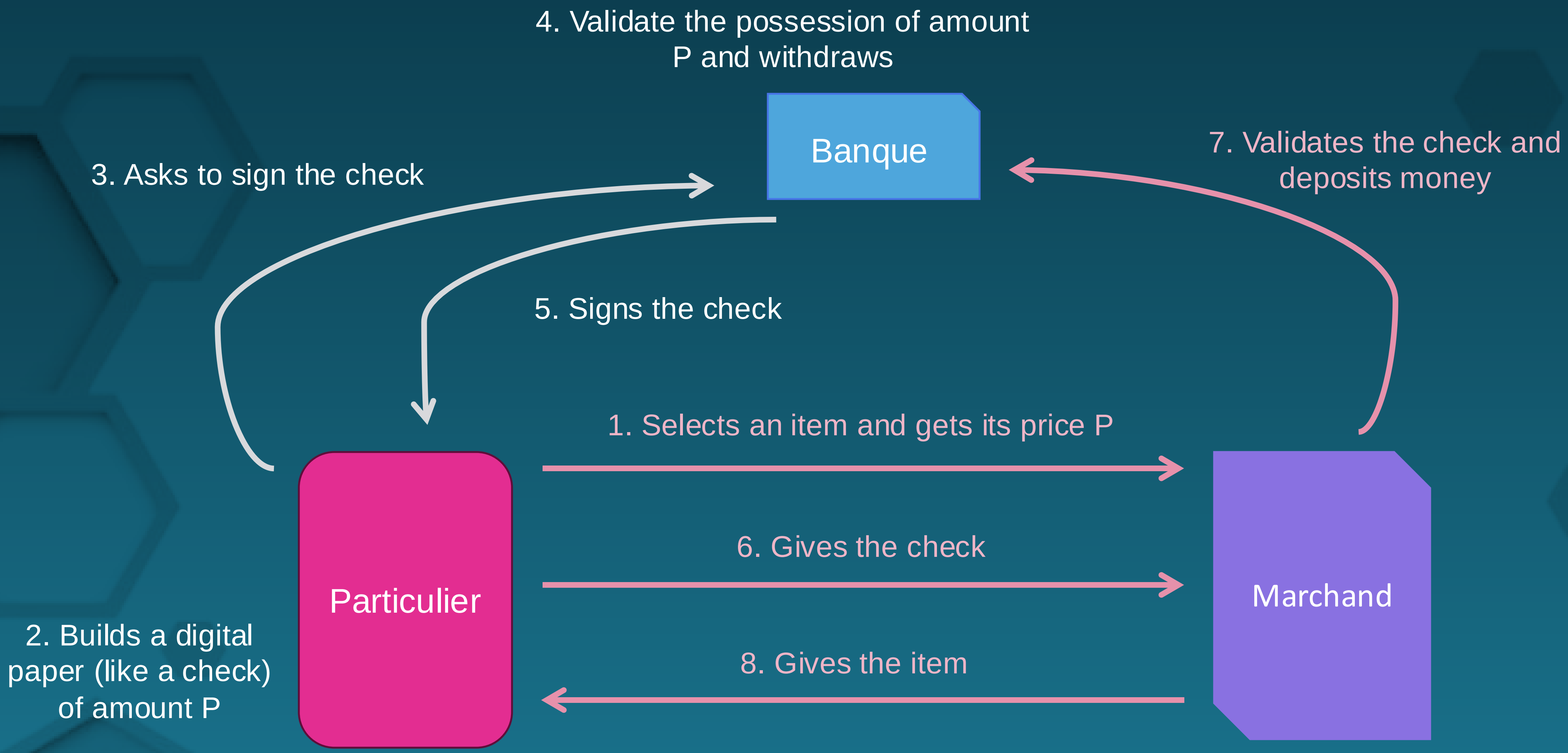
1982 — Blind signatures



Blind Signatures — 1982



Blind Signatures — 1982



4. Validate the possession of amount P and withdraws

3. Asks to sign the check

7. Validates the check and deposits money

5. Signs the check

1. Selects an item and gets its price P

6. Gives the check

8. Gives the item

2. Builds a digital paper (like a check) of amount P

David Chaum — 1982

1989 — Creates DigiCash

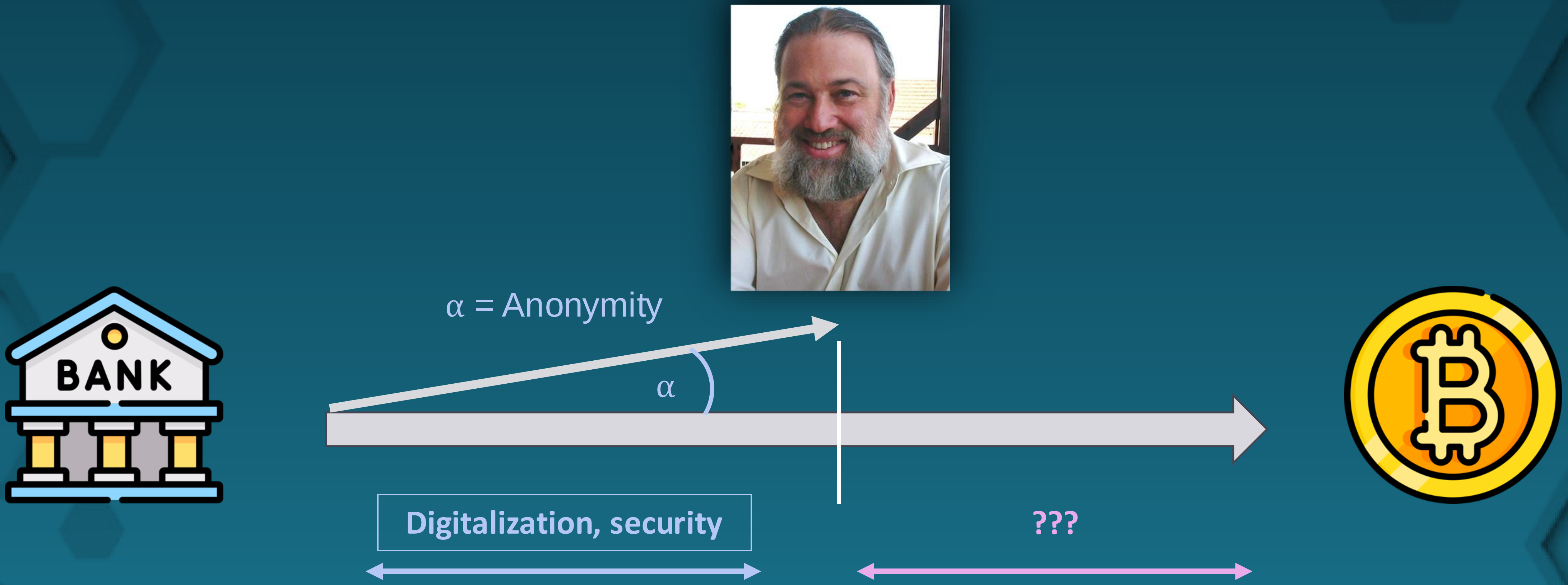
- Software that allows one to withdraw an exact amount of money for a transaction using a digital equivalent of a check
- Implements the blind signature protocol
- Uses “Cyberbucks”
- Partnership with The Mark Twain Bank (Missouri), Deutsche Bank (Allemagne), Crédit Suisse, +3 others

David Chaum — 1982

1998 — Bankruptcy !

- Has known great success, but huge lack of business model
- Paypal is better
- Some people said Chaum’s paranoid behaviour made him refuse important partnerships
- Chaum claims it is an issue of chicken/egg : DigiCash needs merchants to operate, but merchants won’t use it if they have no users

From banks to cryptocurrencies



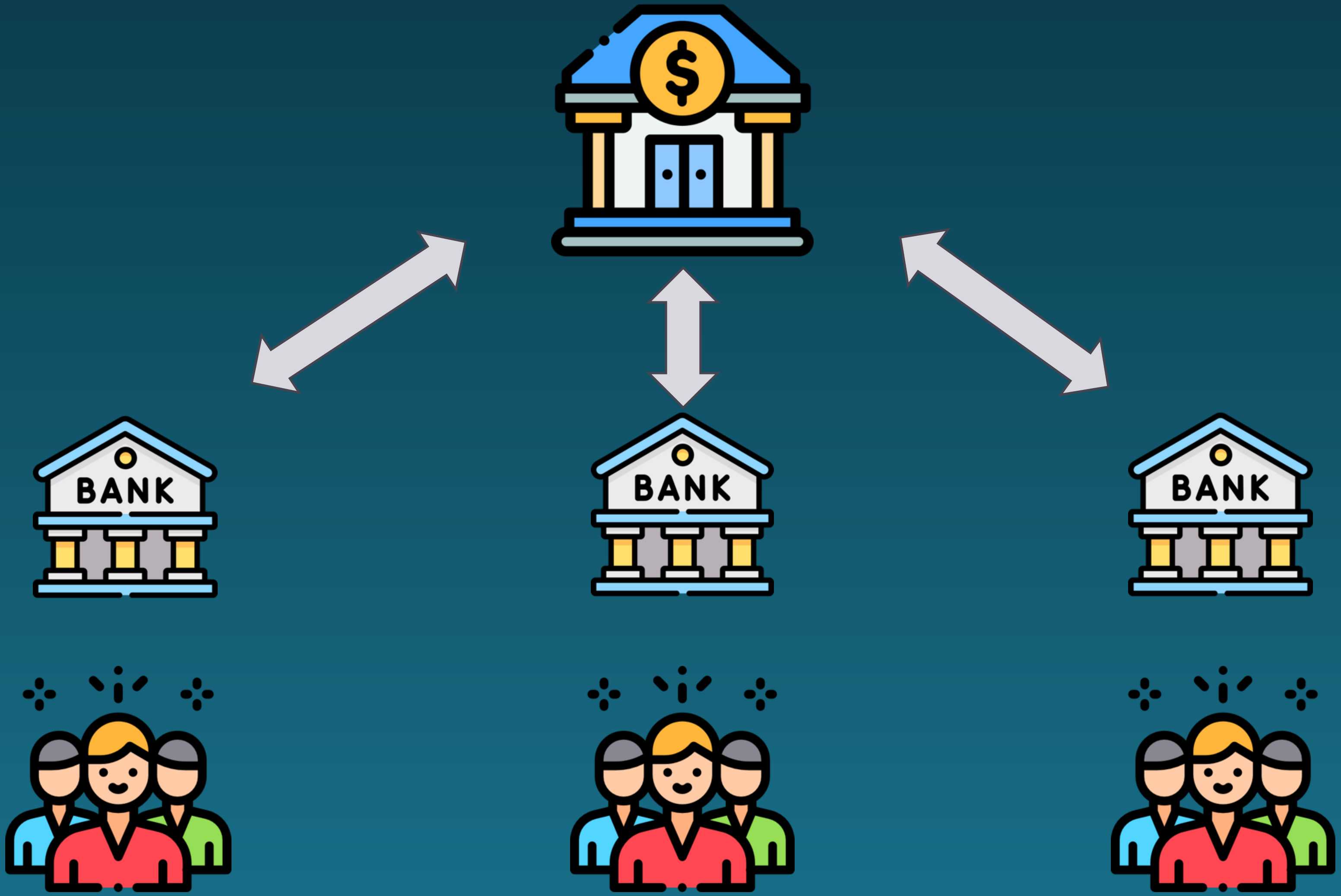
α = Anonymity

α

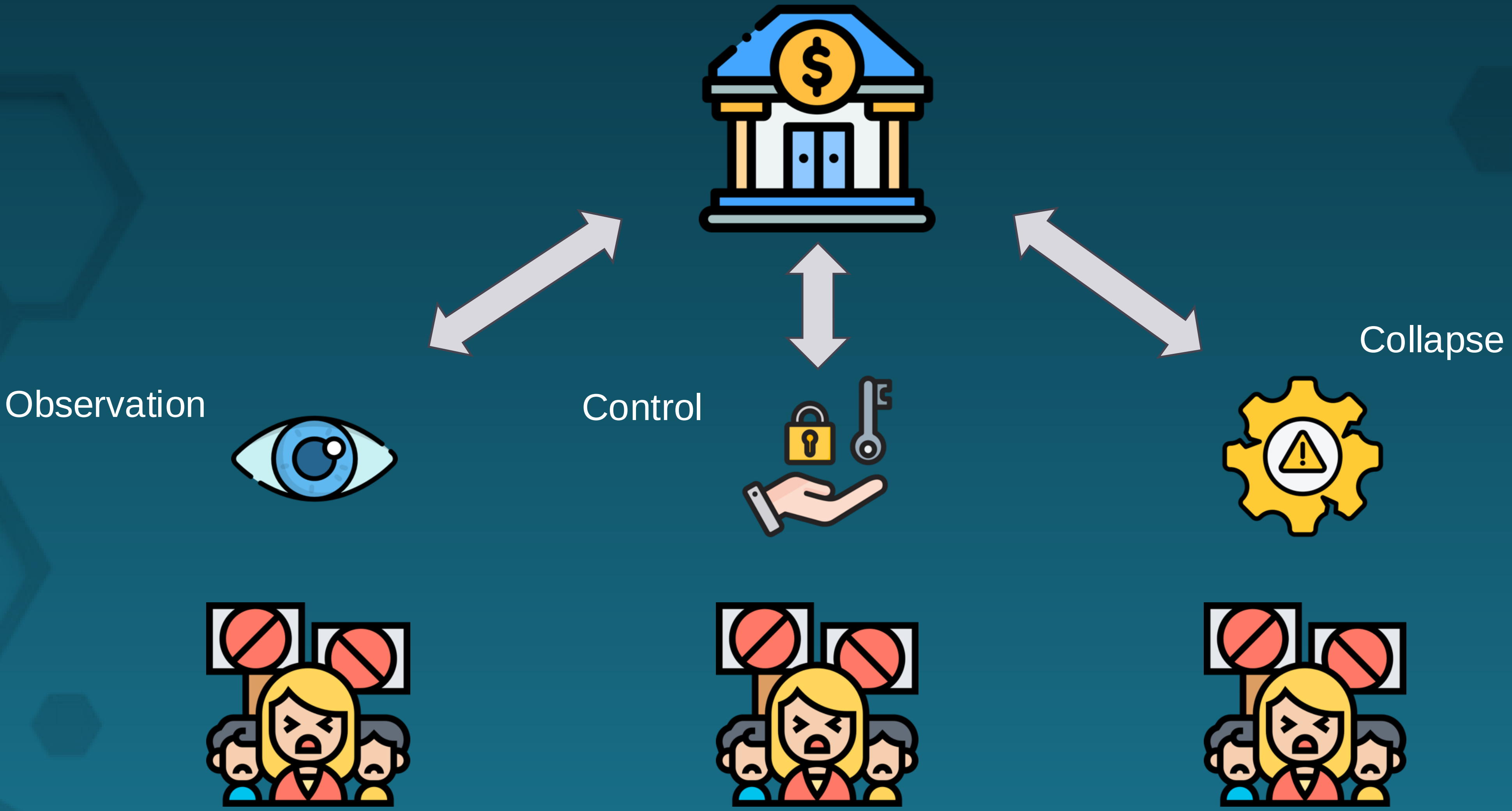
Digitalization, security

???

Centralized economy



Centralized economy

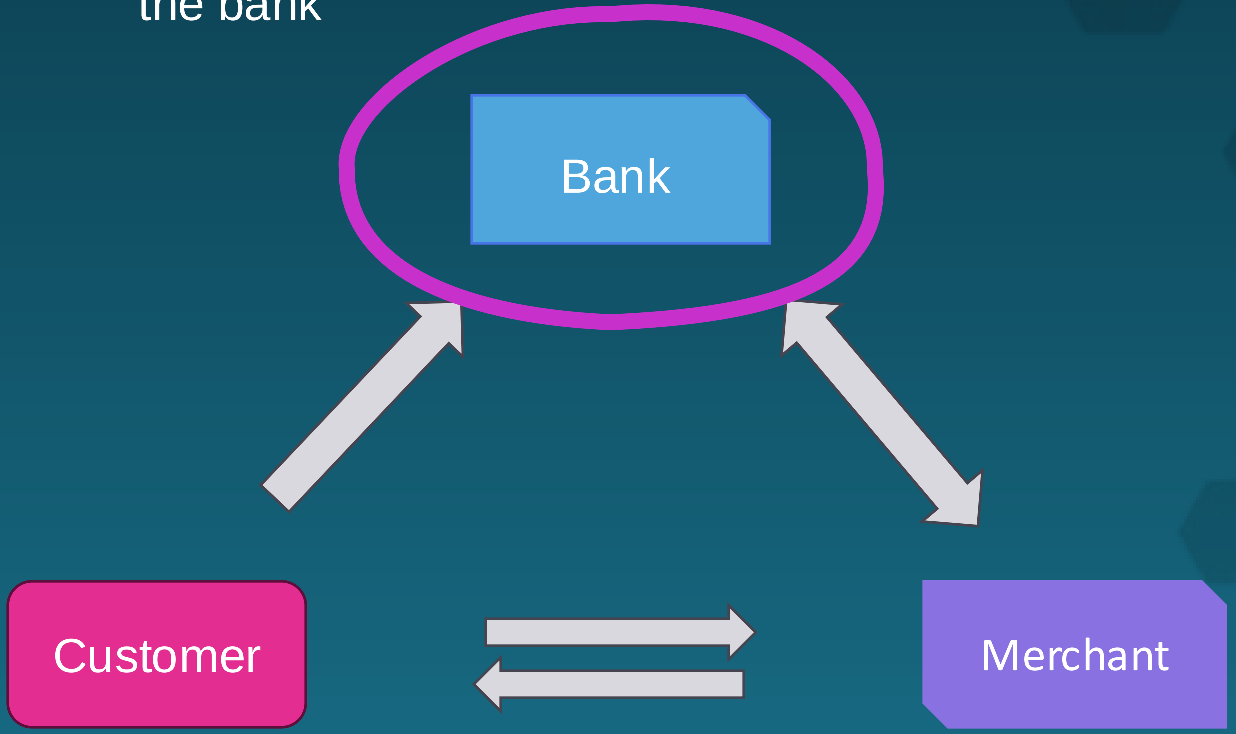


Observation

Control

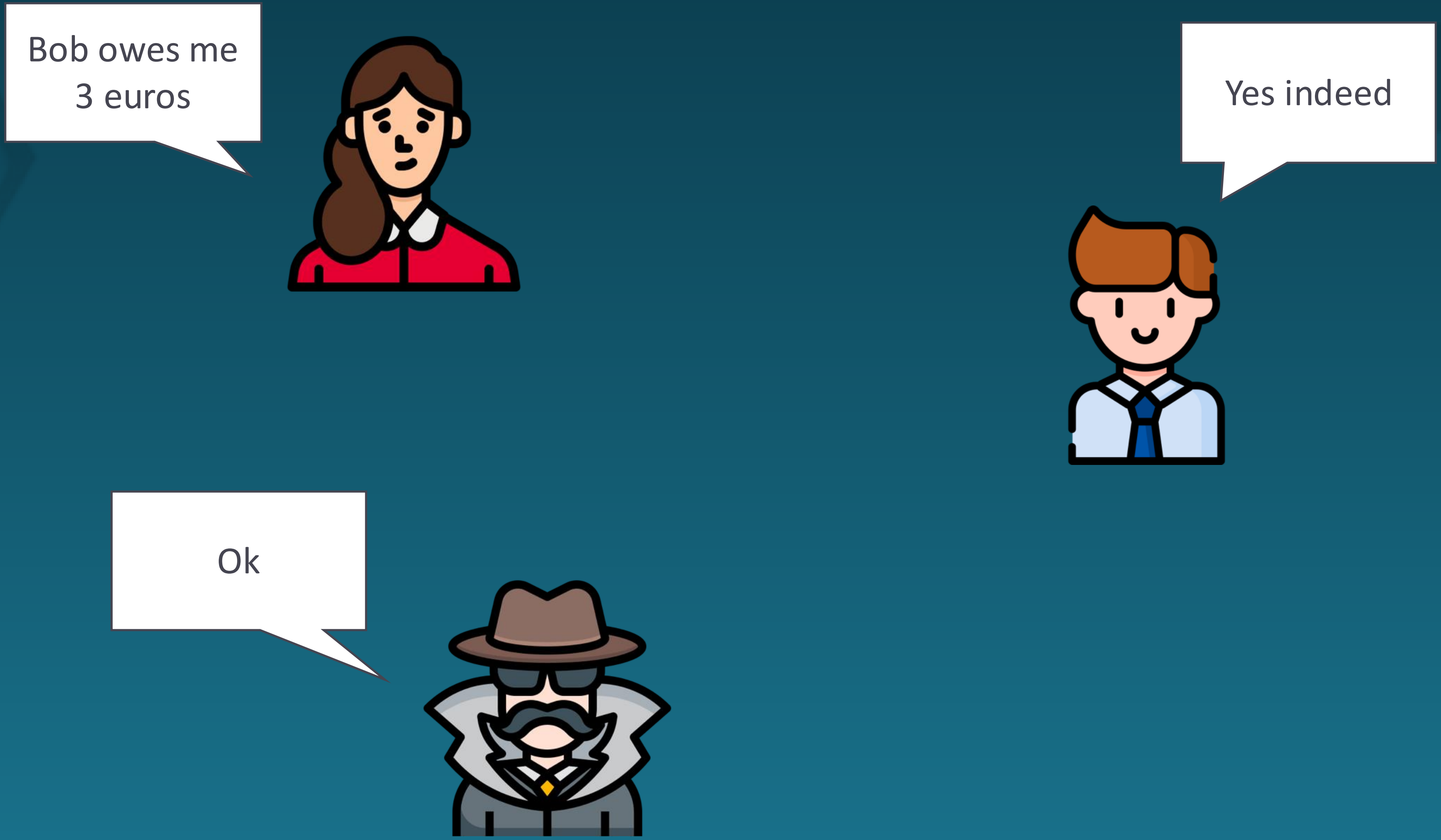
Collapse

David Chaum’s model — A paradox ?

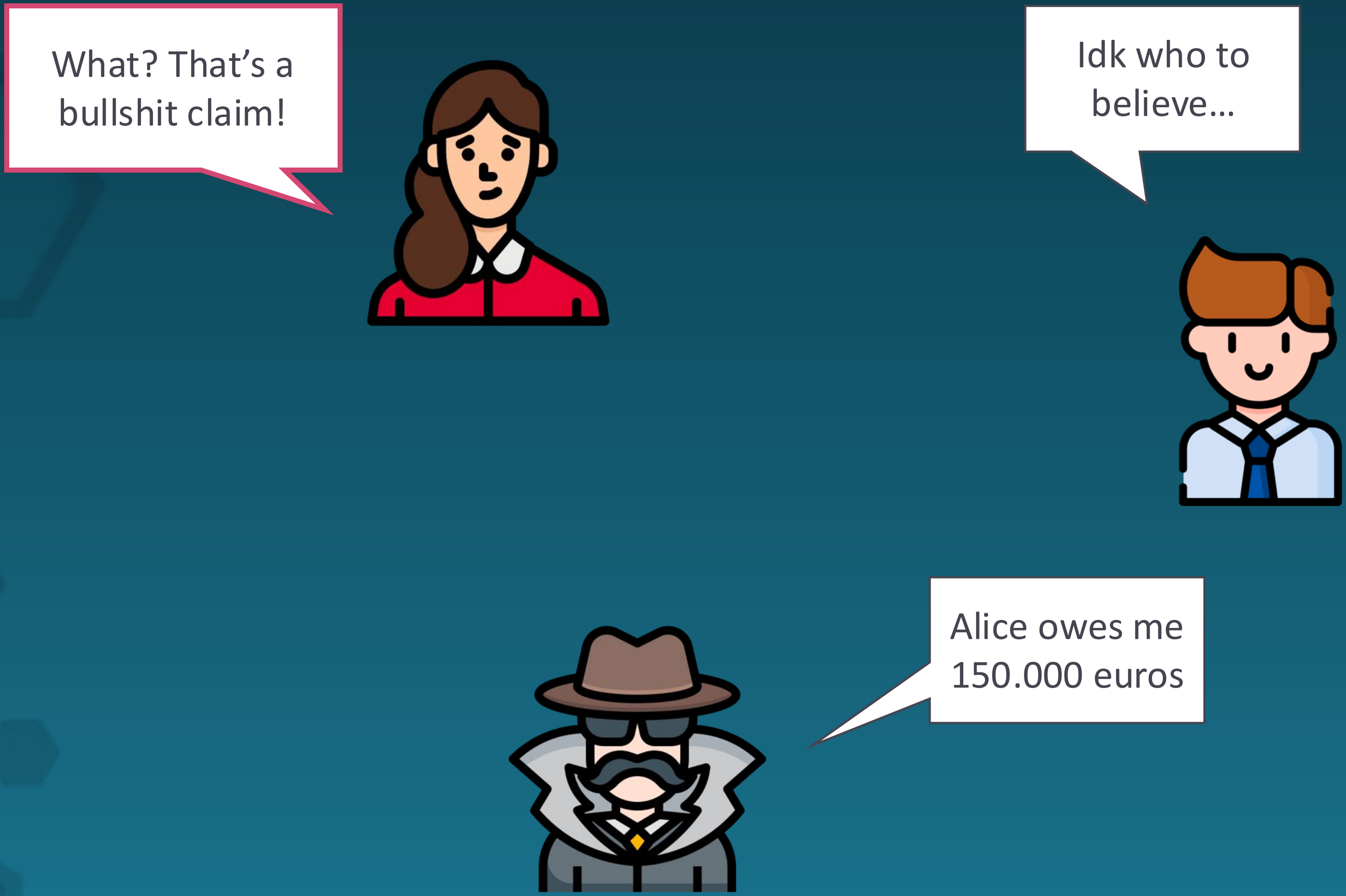


Centralized around the bank

The need to centralize



The need to centralize



What? That’s a bullshit claim!

Idk who to believe…

Alice owes me 150.000 euros

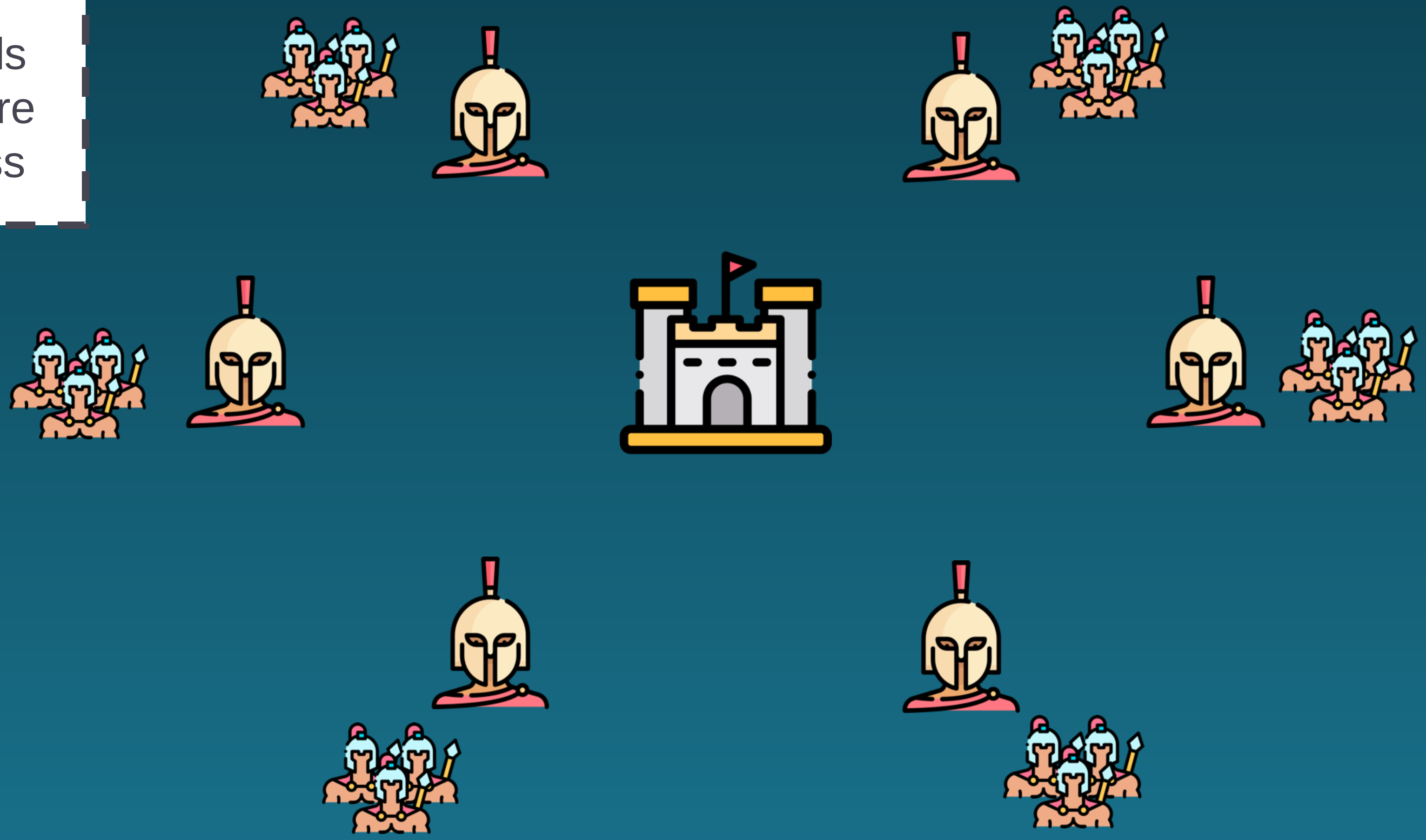
Byzantine Fault Tolerance (BFT)

A BFT system has to agree on a truth even if some individuals are either faulty or broken

Leslie Lamport, Robert Shostak and Marshall Pease — 1982

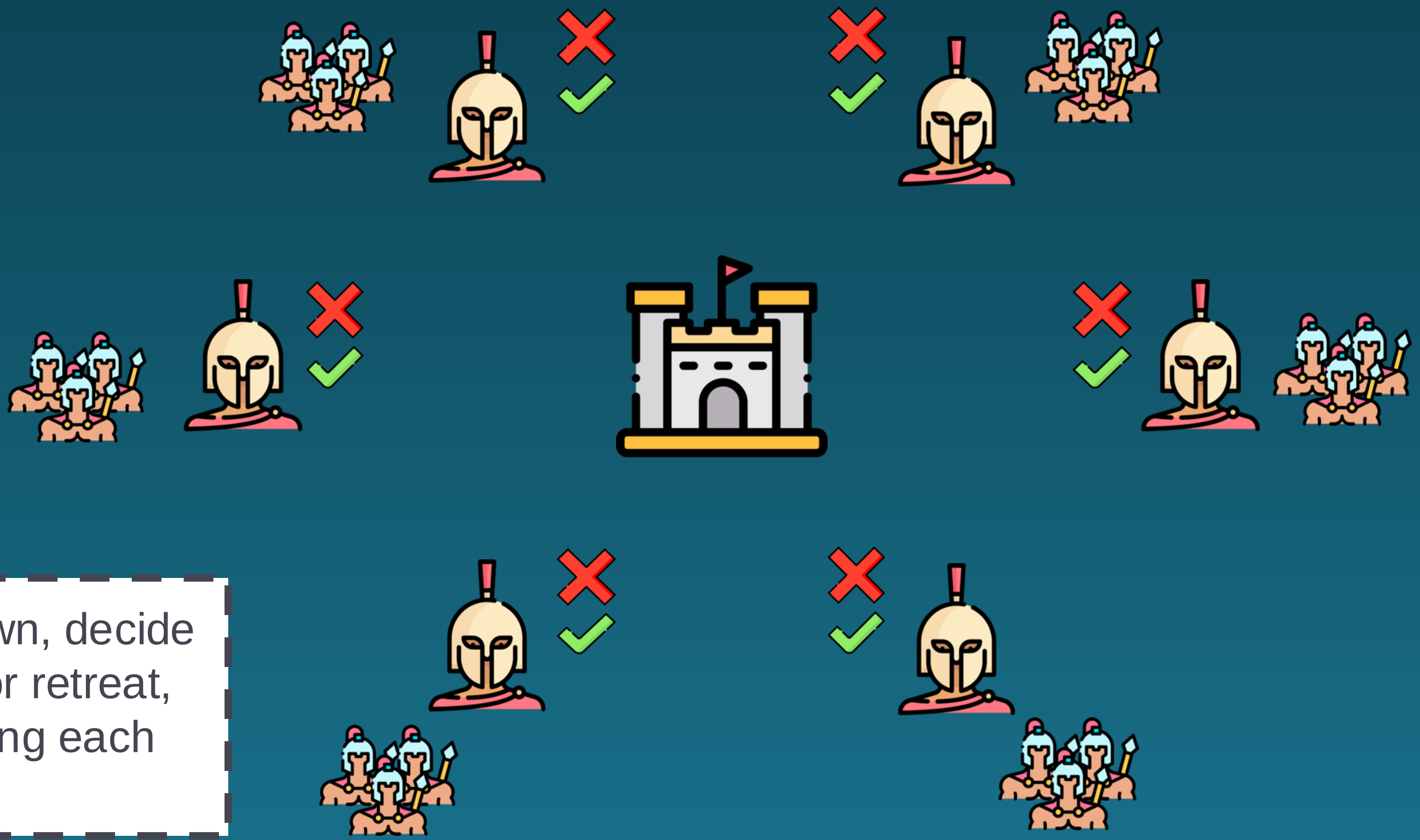
Byzantine generals problem

Byzantine generals (with their army) are attacking a fortress



Leslie Lamport, Robert Shostak and Marshall Pease — 1982

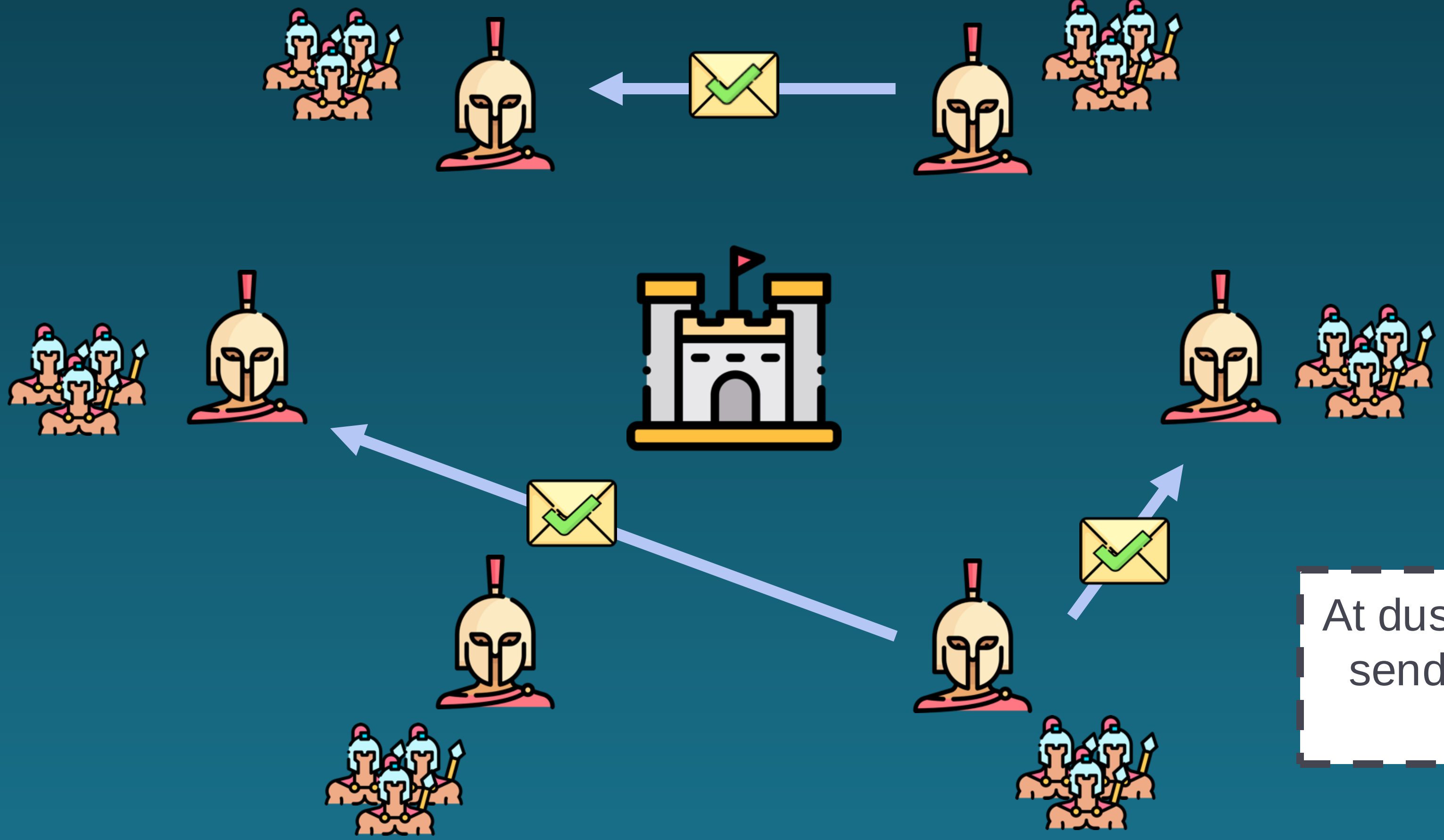
Byzantine generals problem



They must, at dawn, decide either to attack or retreat, without consulting each other

Leslie Lamport, Robert Shostak and Marshall Pease — 1982

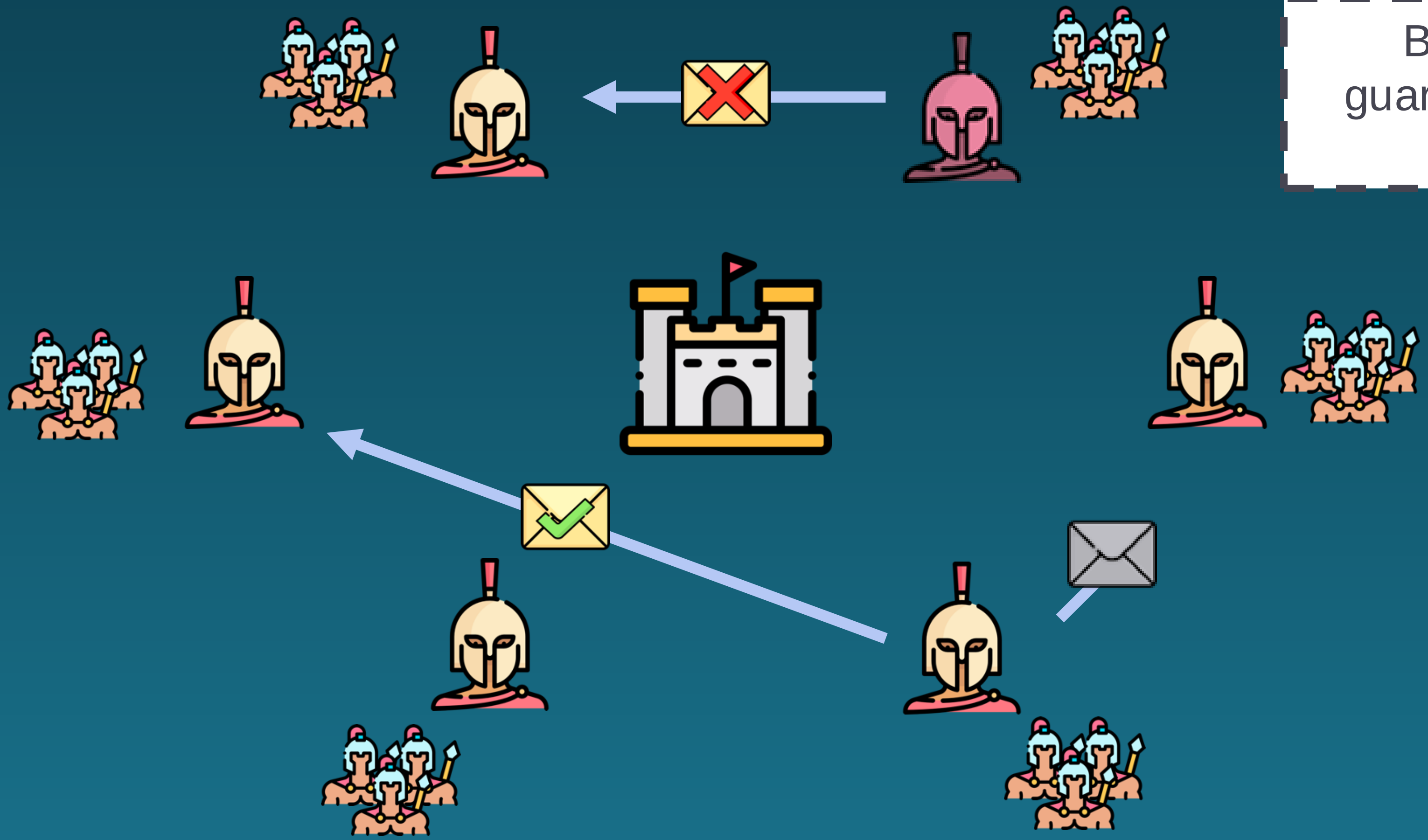
Byzantine generals problem



At dusk the day before, they send each other letters to tell their intent

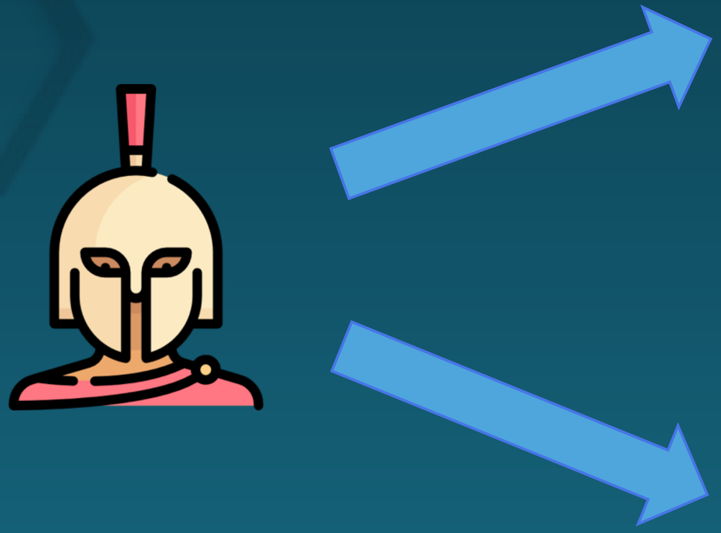
Leslie Lamport, Robert Shostak and Marshall Pease — 1982

Byzantine generals problem



But there is no guarantee a intent is genuine…

Problem solving



Barbara Liskov and Miguel Castro (1990)

Exact solution, but max 1/3 faulty

Exponential time…

Approximated solution ?

Probabilistic solution

Satoshi Nakamoto — 2008

Satoshi Nakamoto — 2008

31 October 2008 — “Bitcoin: A Peer-to-Peer Electronic Cash System”

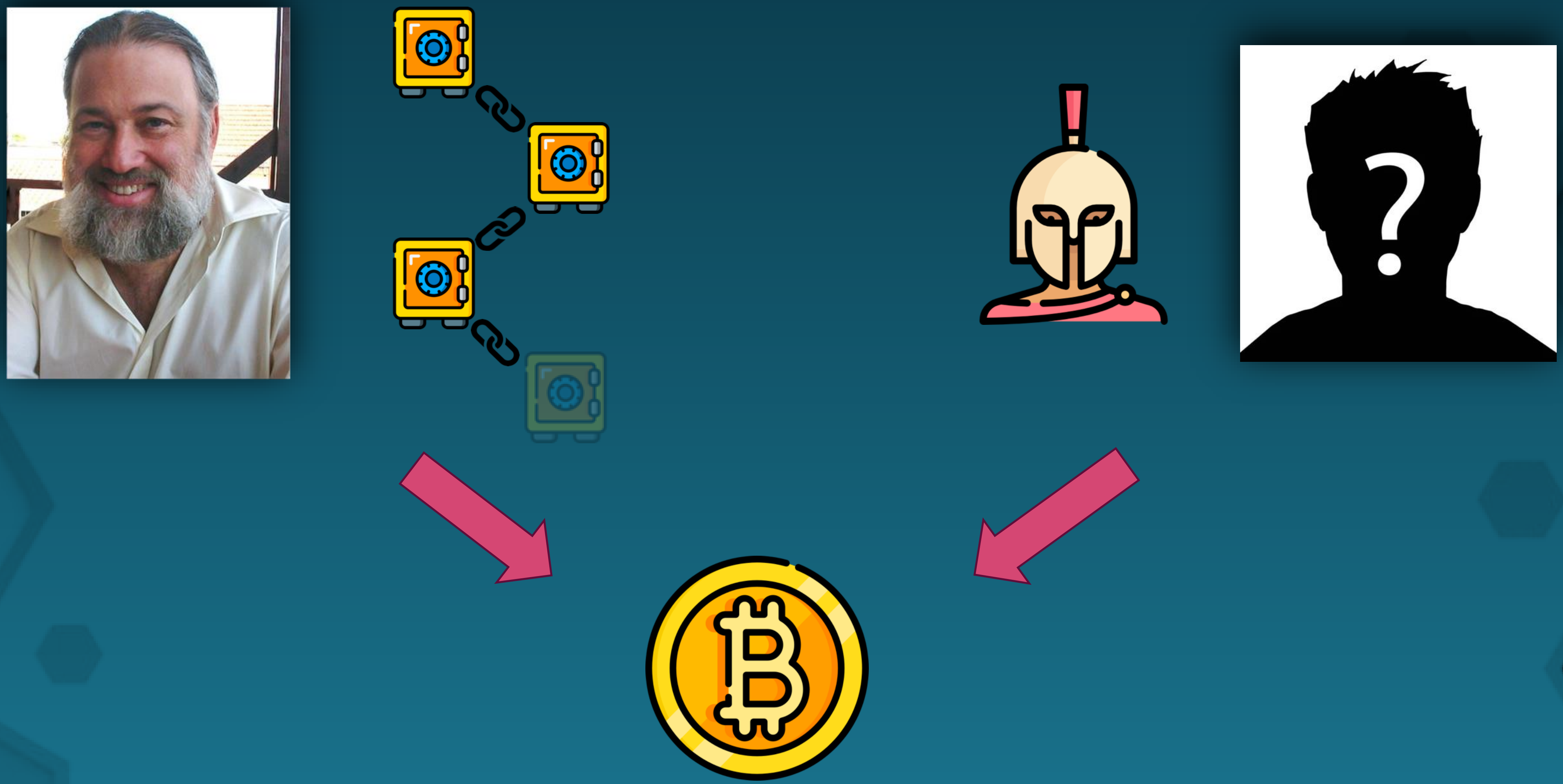
3 January 2009 — Launching Bitcoin (genesis block)

22 May 2010 — first bitcoin purchase (Two pizzas for 10.000 BTC)

September 2021 — Statue of Satoshi Nakamoto in Budapest

bitcoin.org

Birth of Blockchain technology

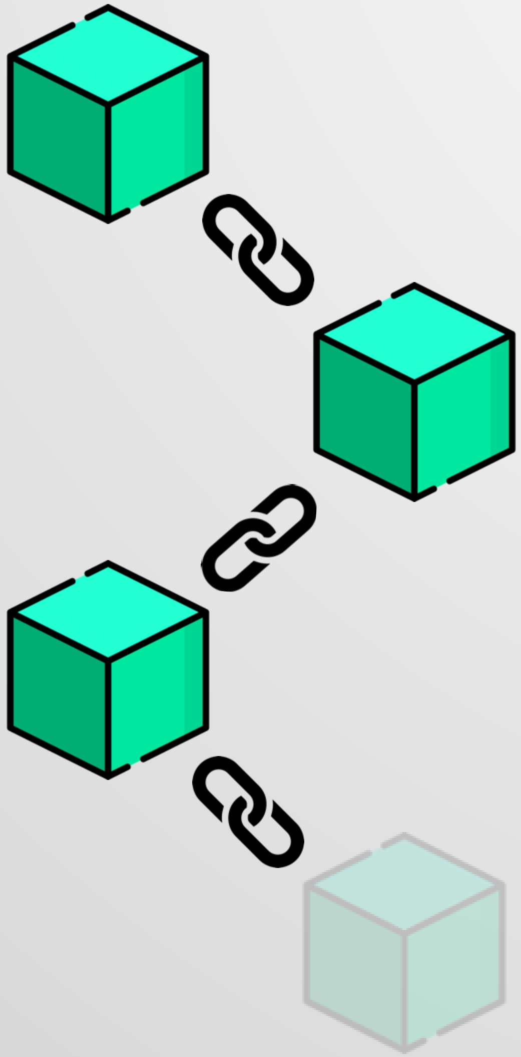


Blockchain ?

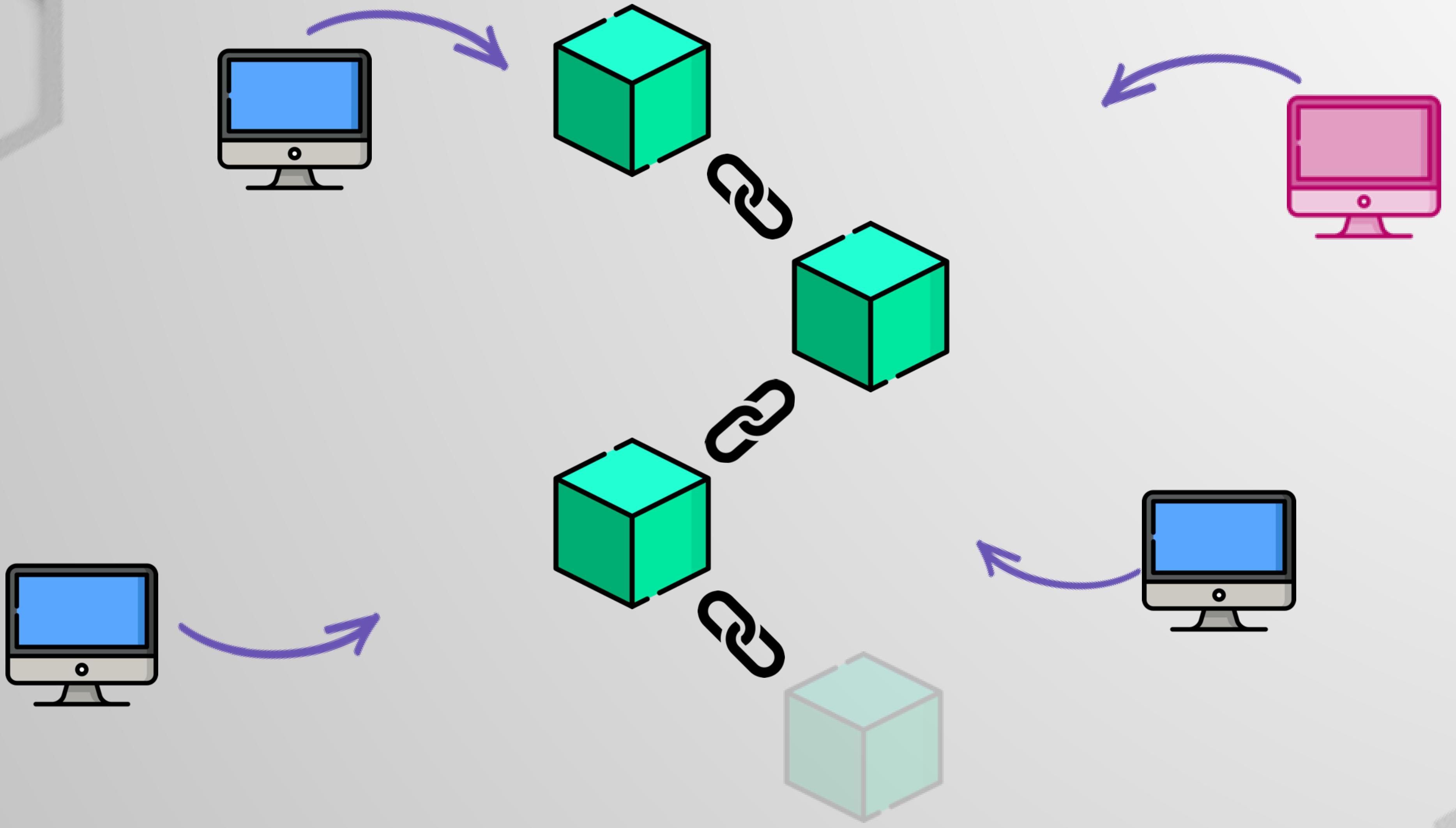
Block = Block

Chain = Chain

Chain of blocks

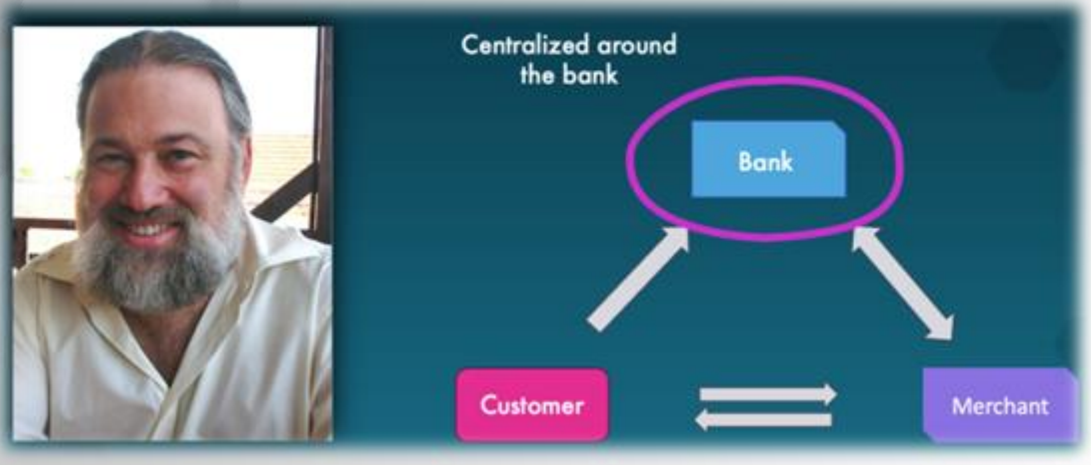


Blockchain ?



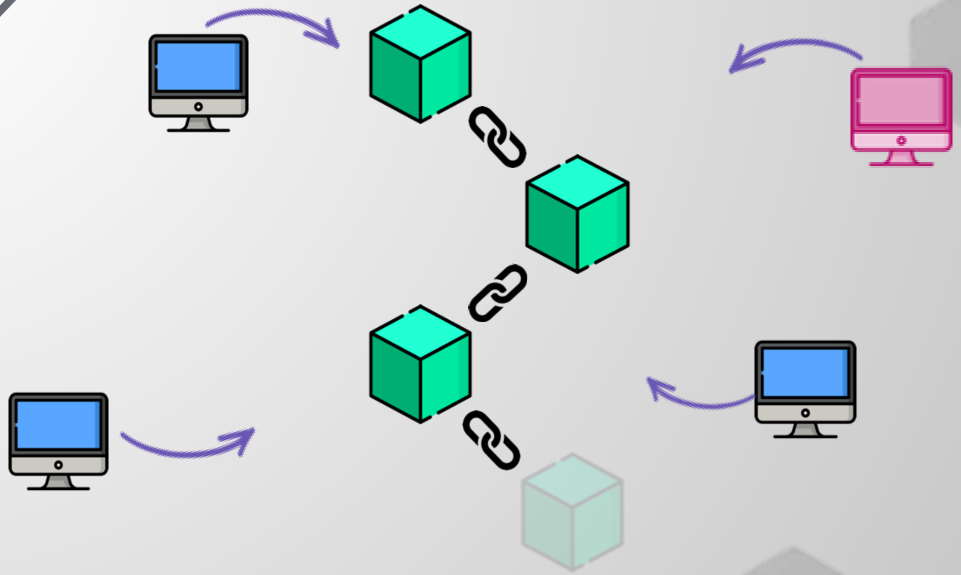
Miracle ?

Decentralization

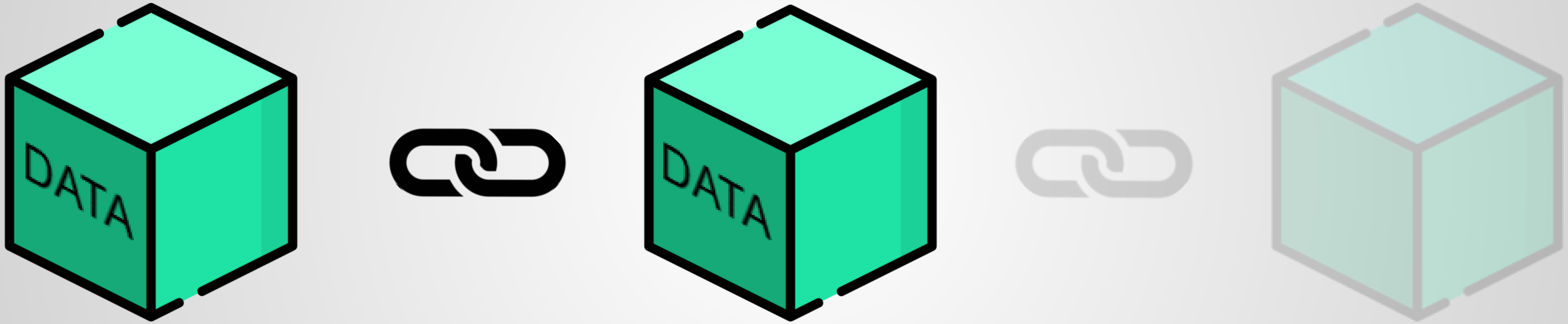


The bank is a mediator and operates at full control over the transaction

Nobody owns full control

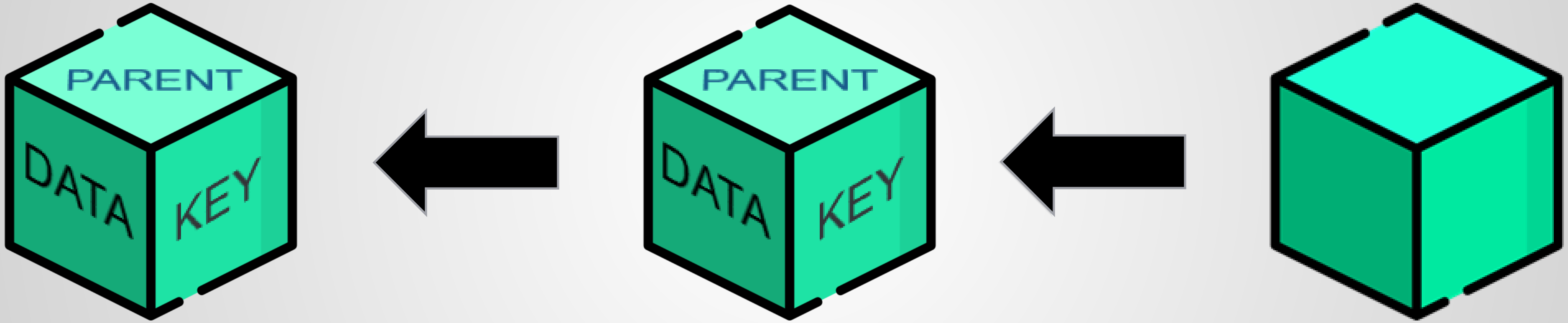


Concrete



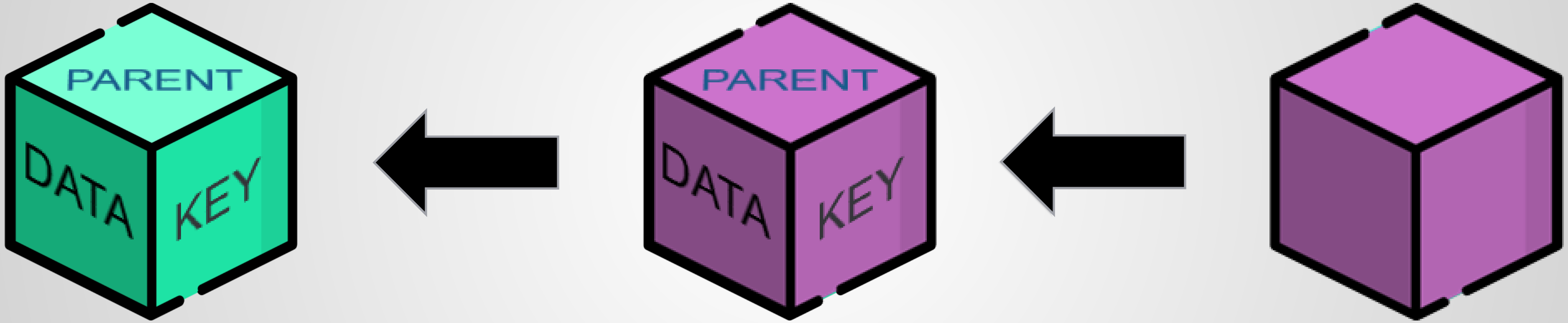
A data storage organized under the shape of a chain of blocks

Concrete



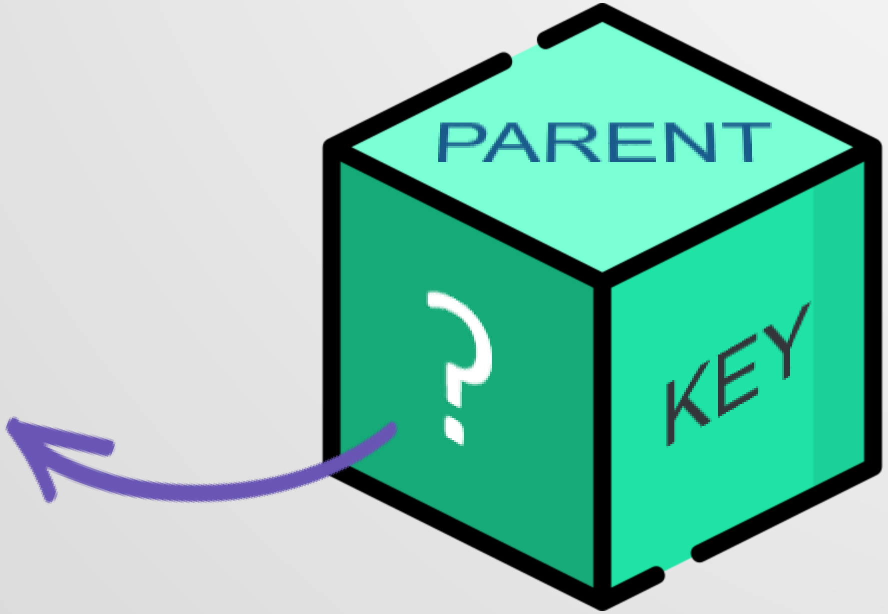
Every block is pointing towards its predecessor

Concrete



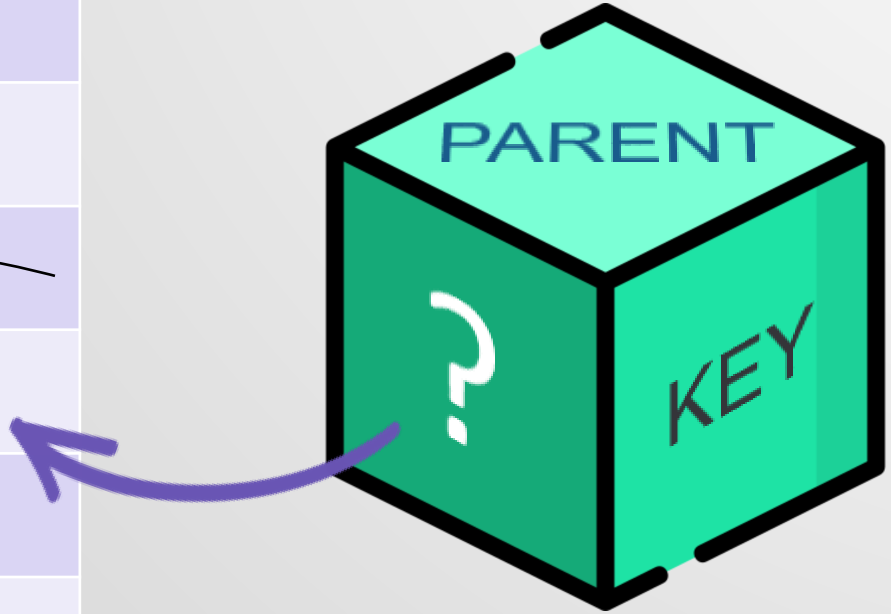
A cryptography system invalidates all blocks following a corrupted block

The famous “Ledger”

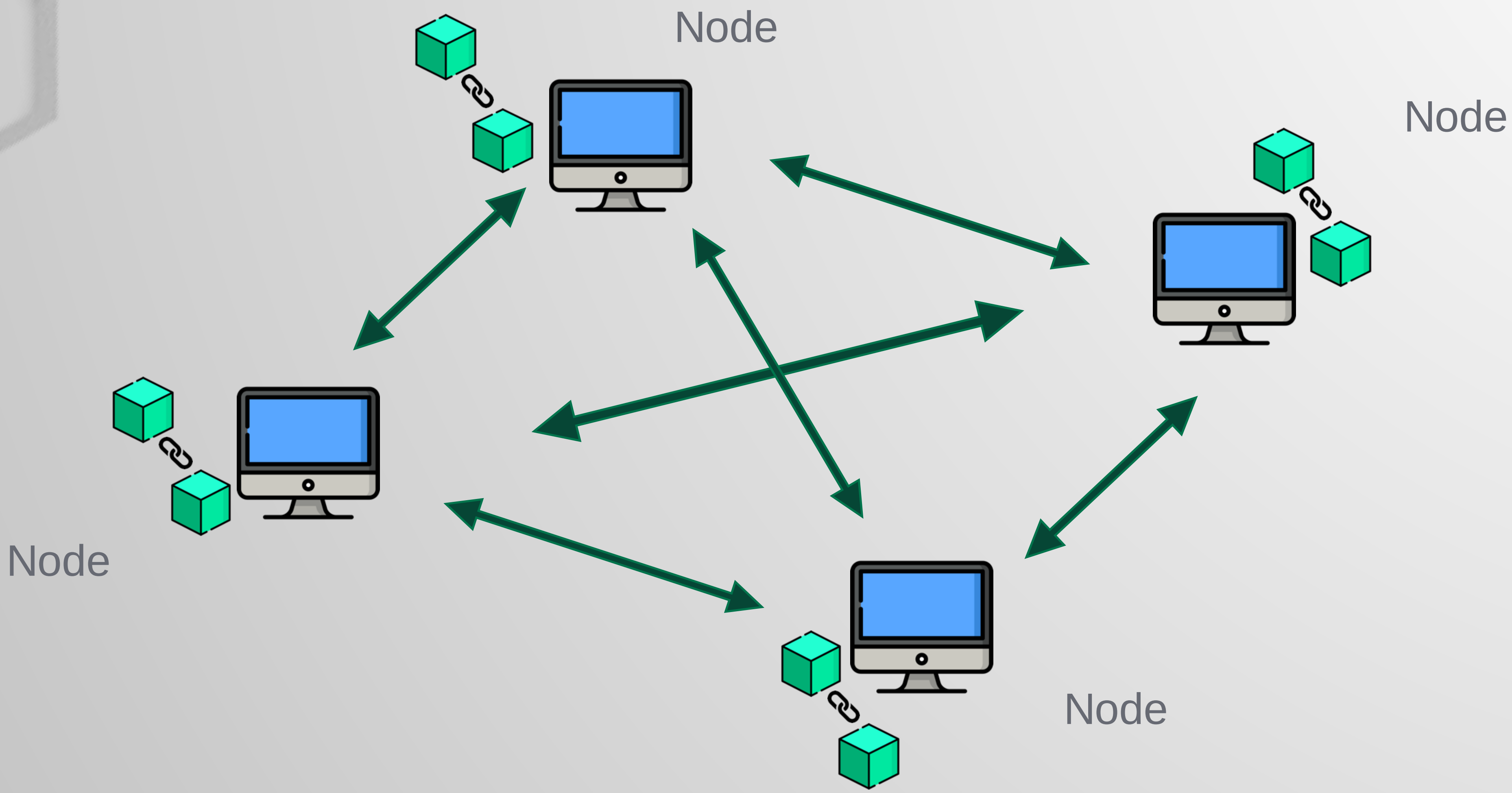


The famous “Ledger”

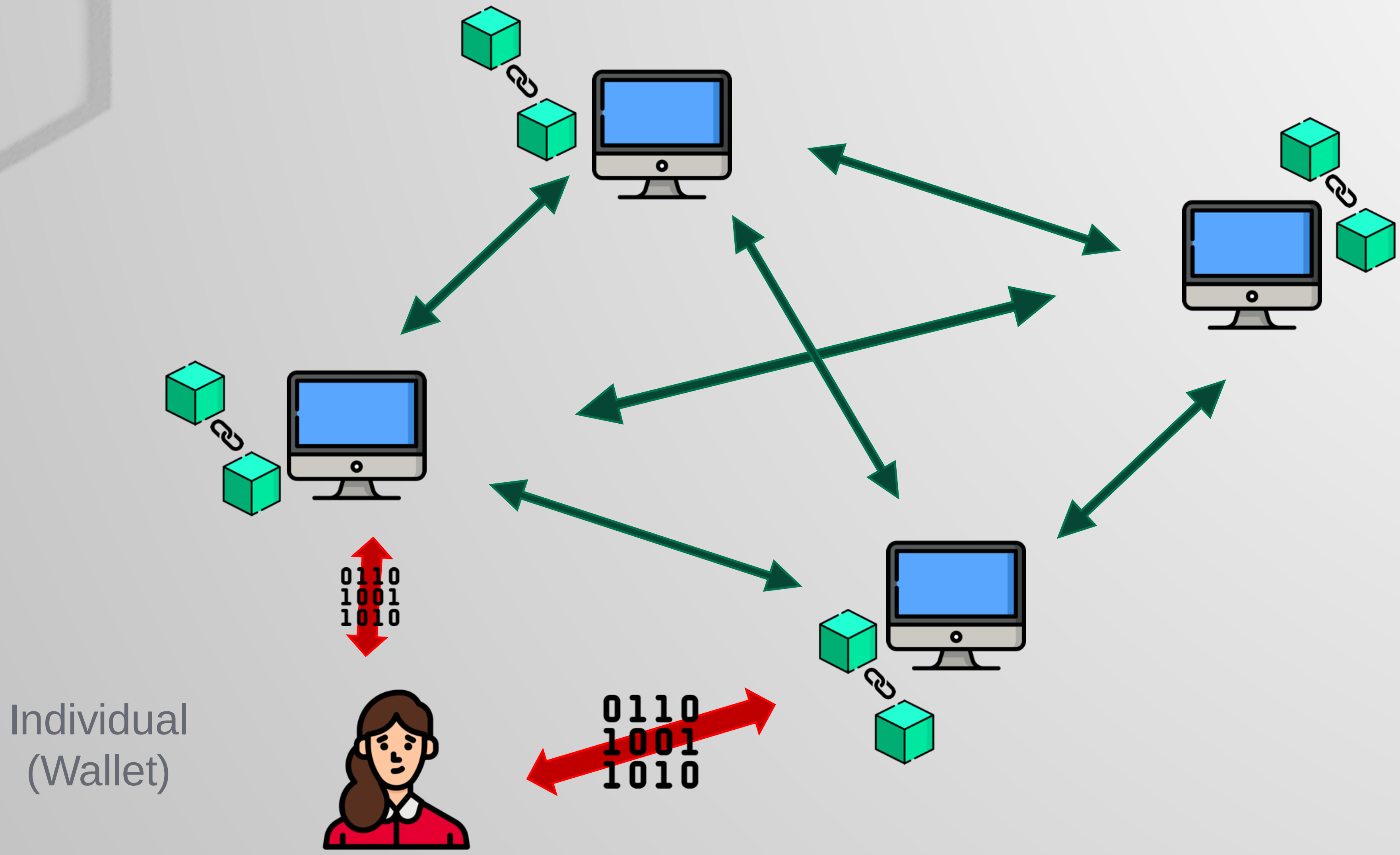
Name	Data	Signature
Alice	…	
Alice	…	
Bob	…	



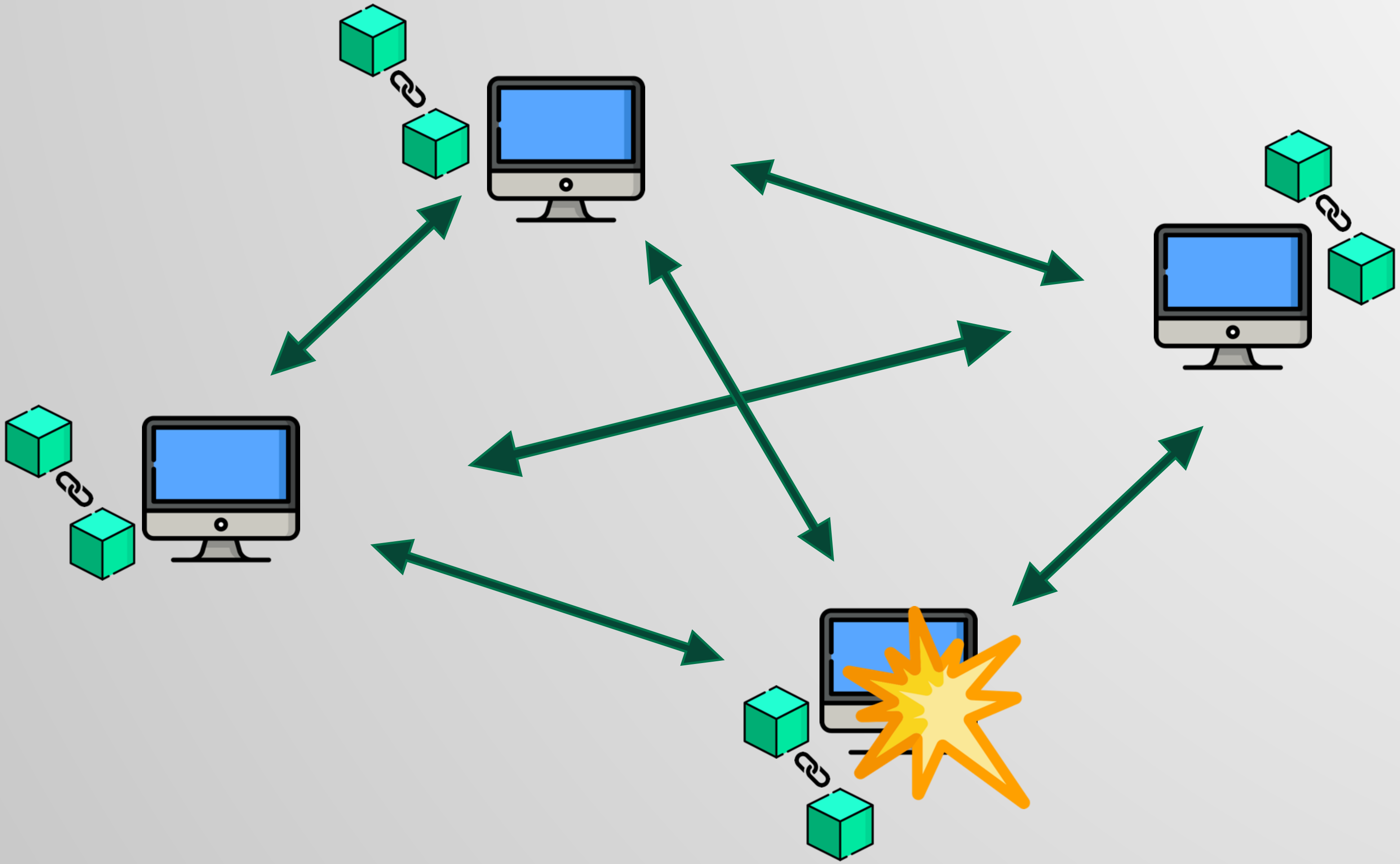
“Distributed” database



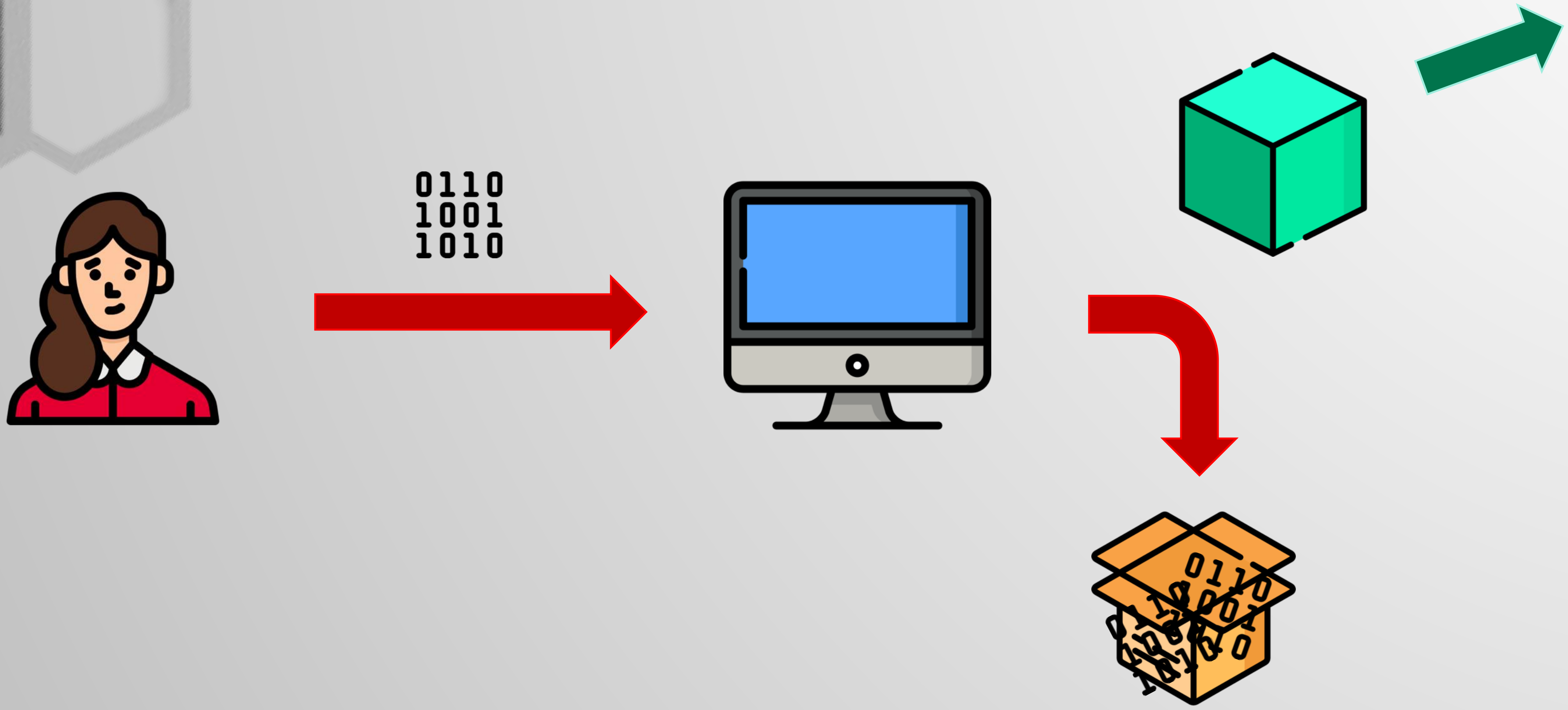
“Distributed” database



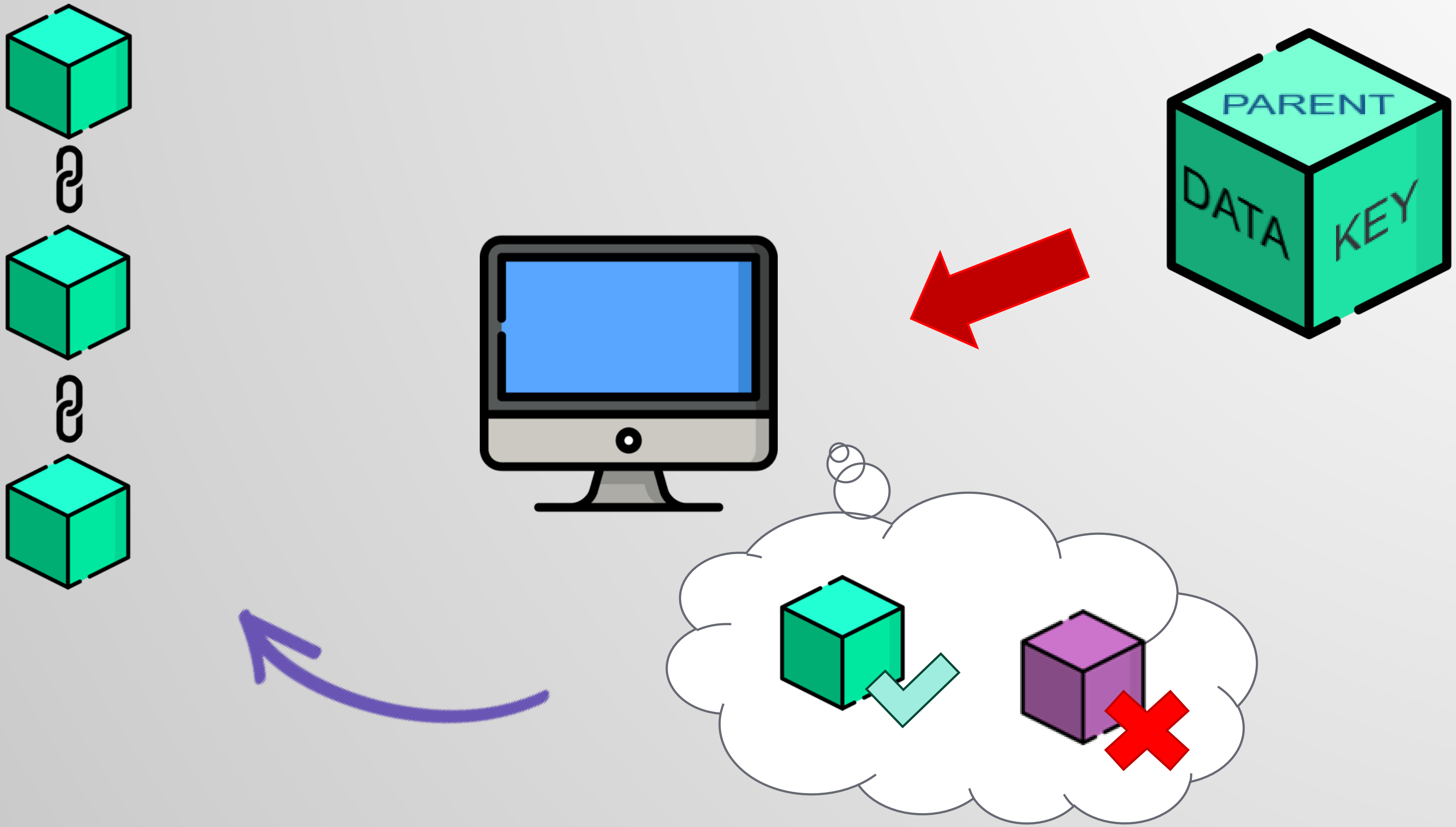
“Distributed” database



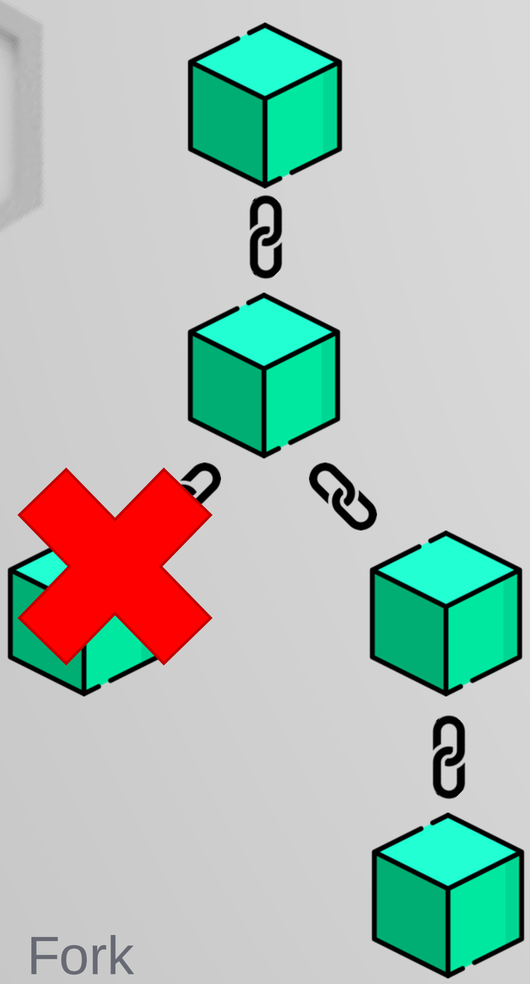
Synchronisation between “Nodes”



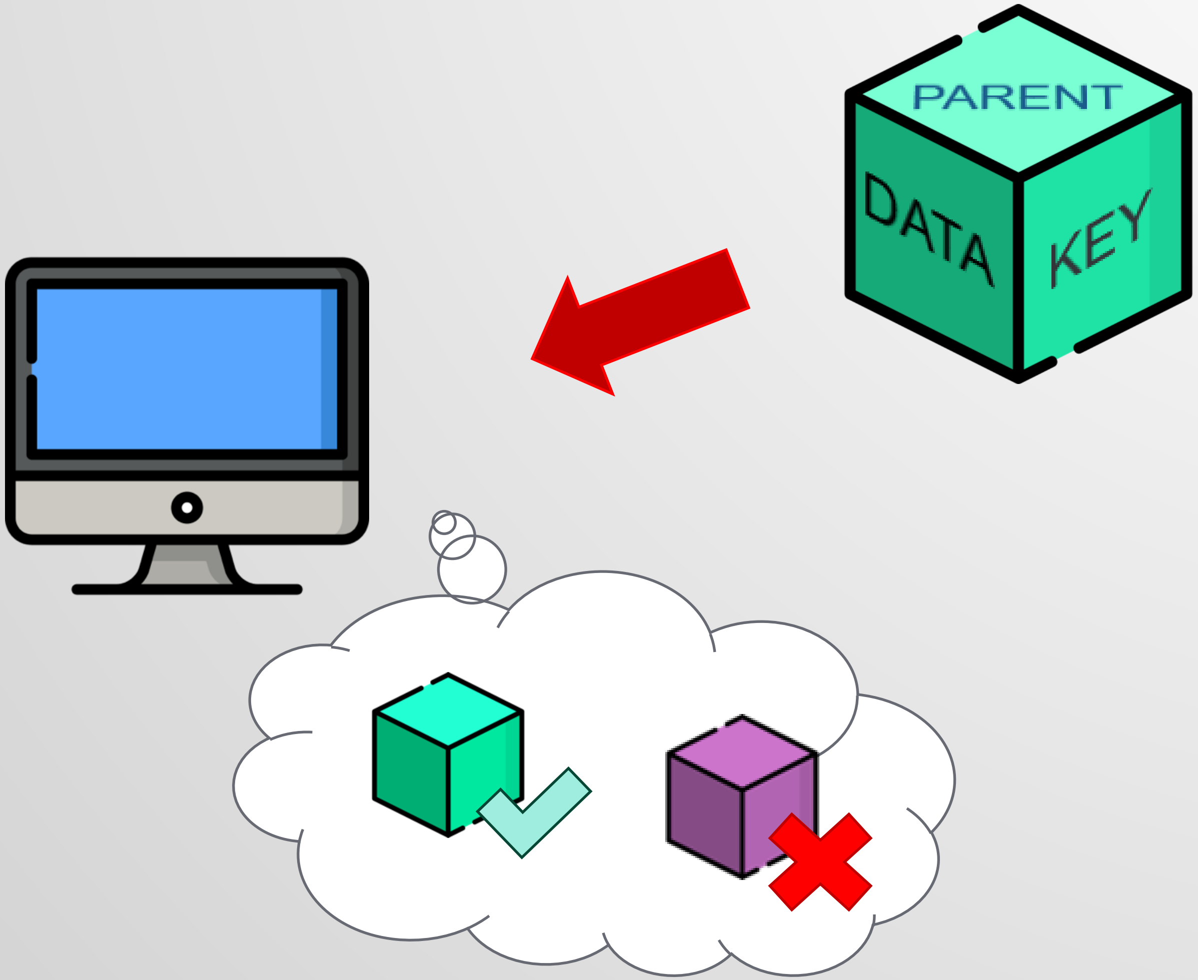
Synchronisation between "Nodes"



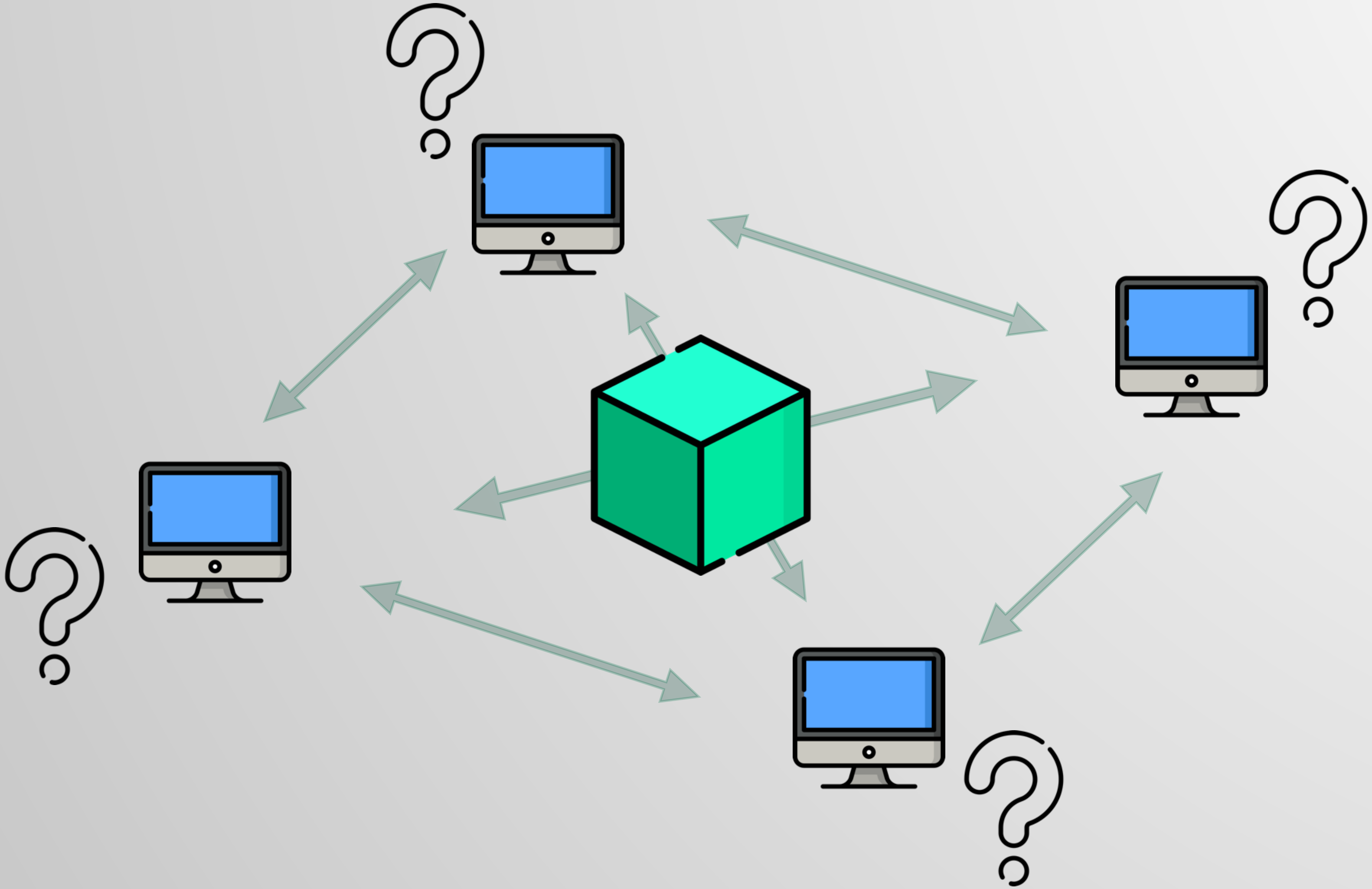
Synchronisation between “Nodes”



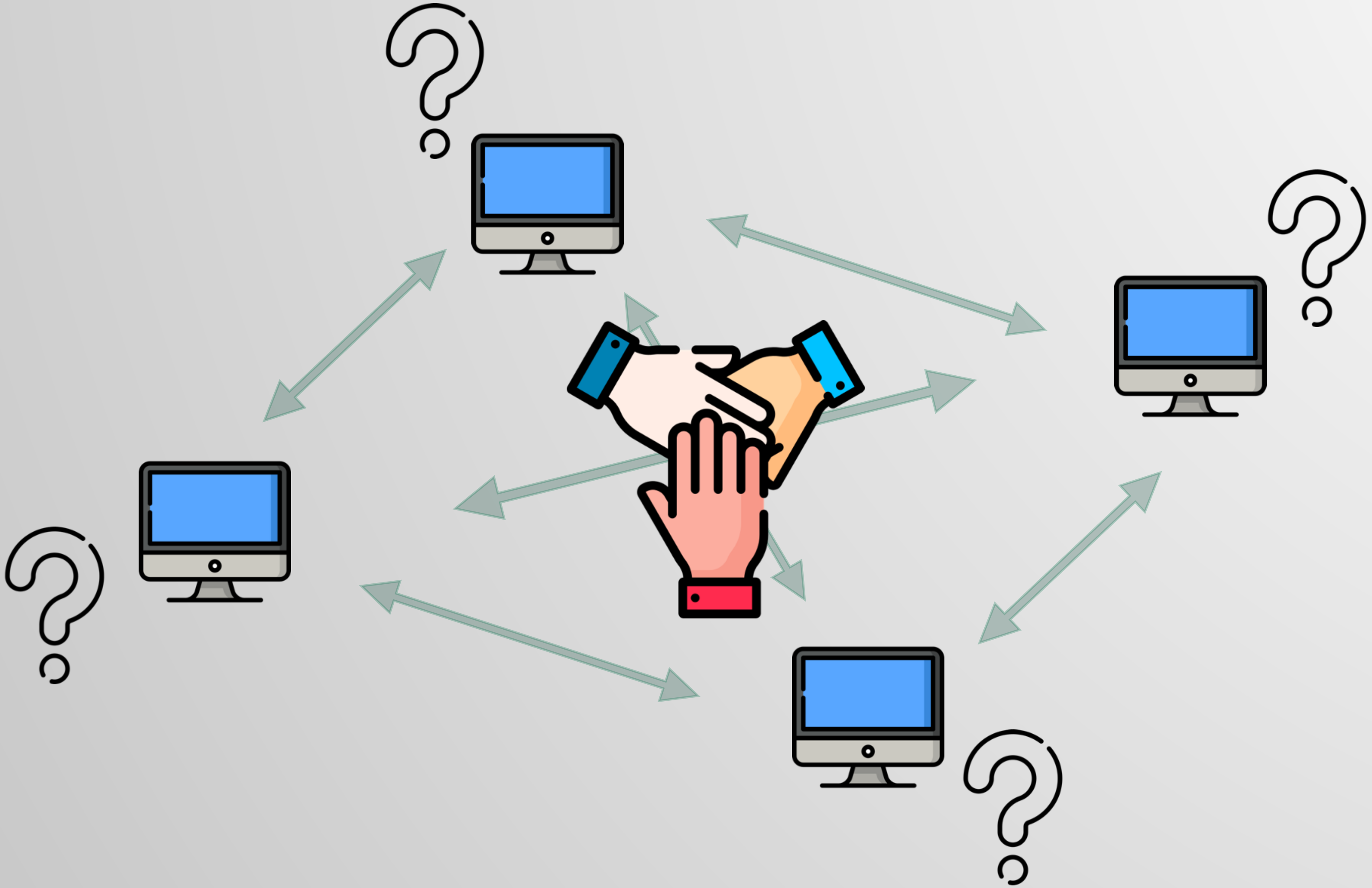
Fork



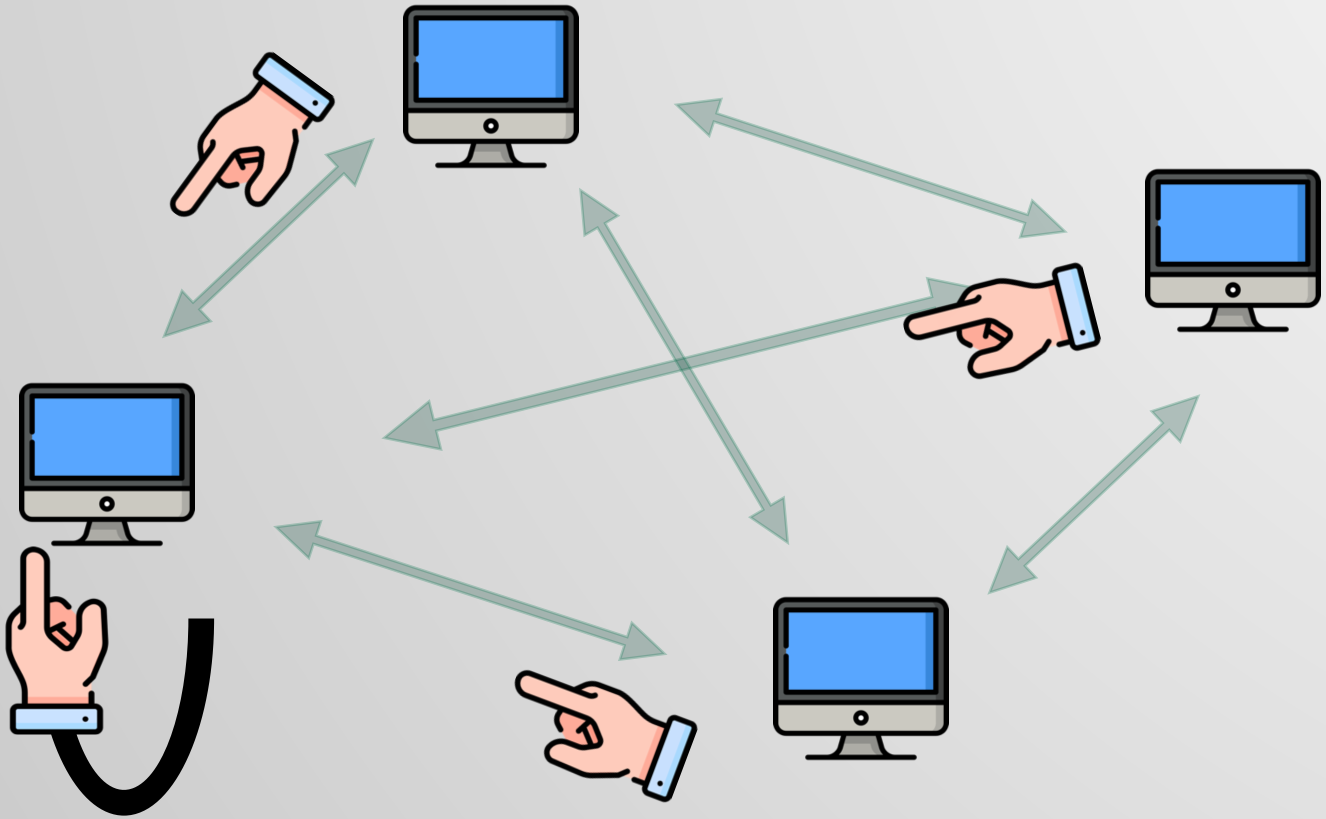
Consensus



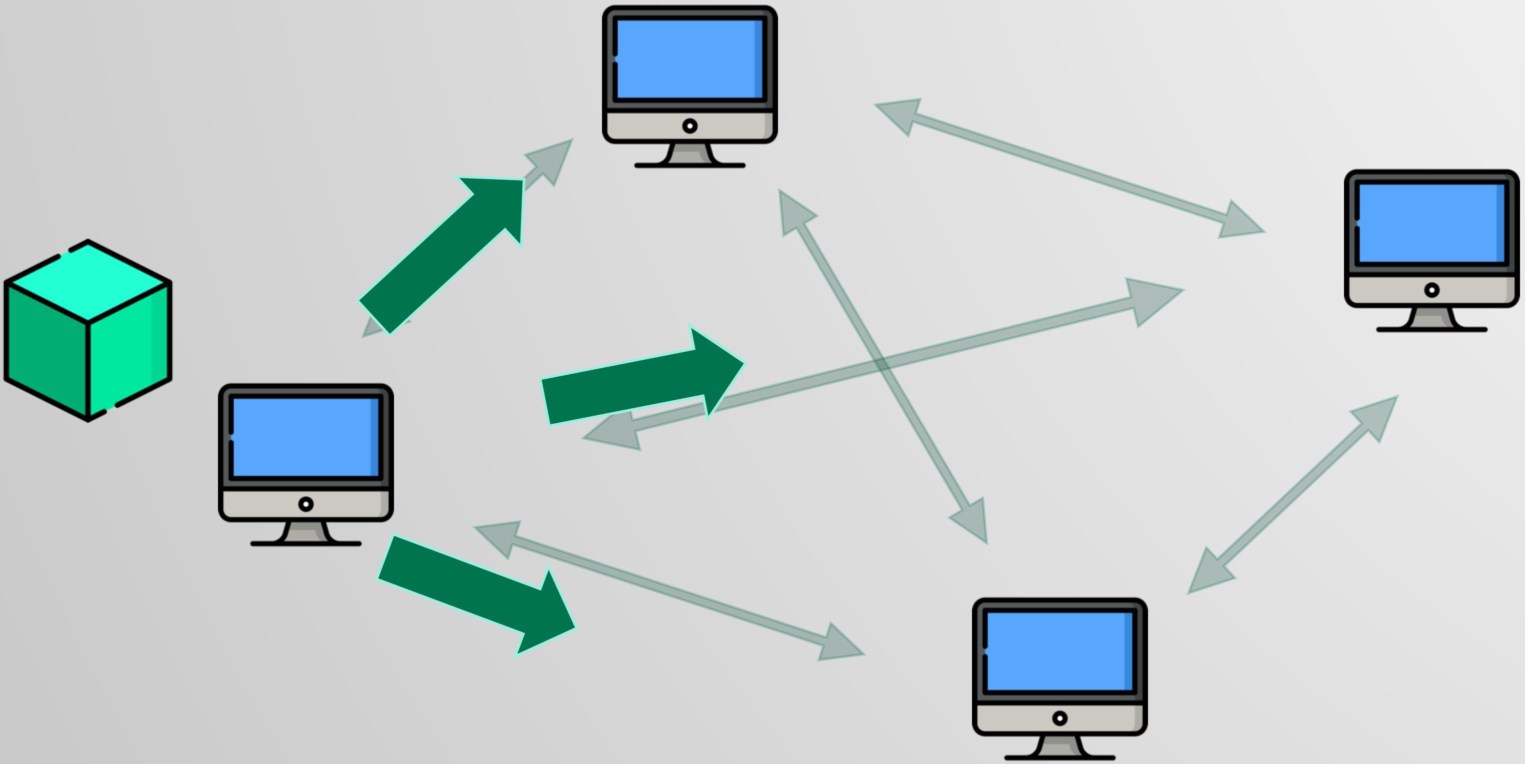
Consensus



Consensus

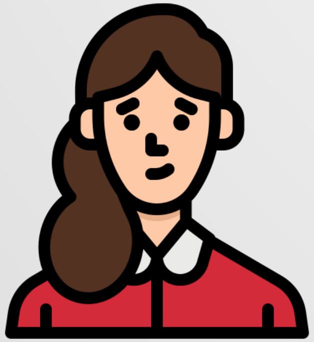


Consensus



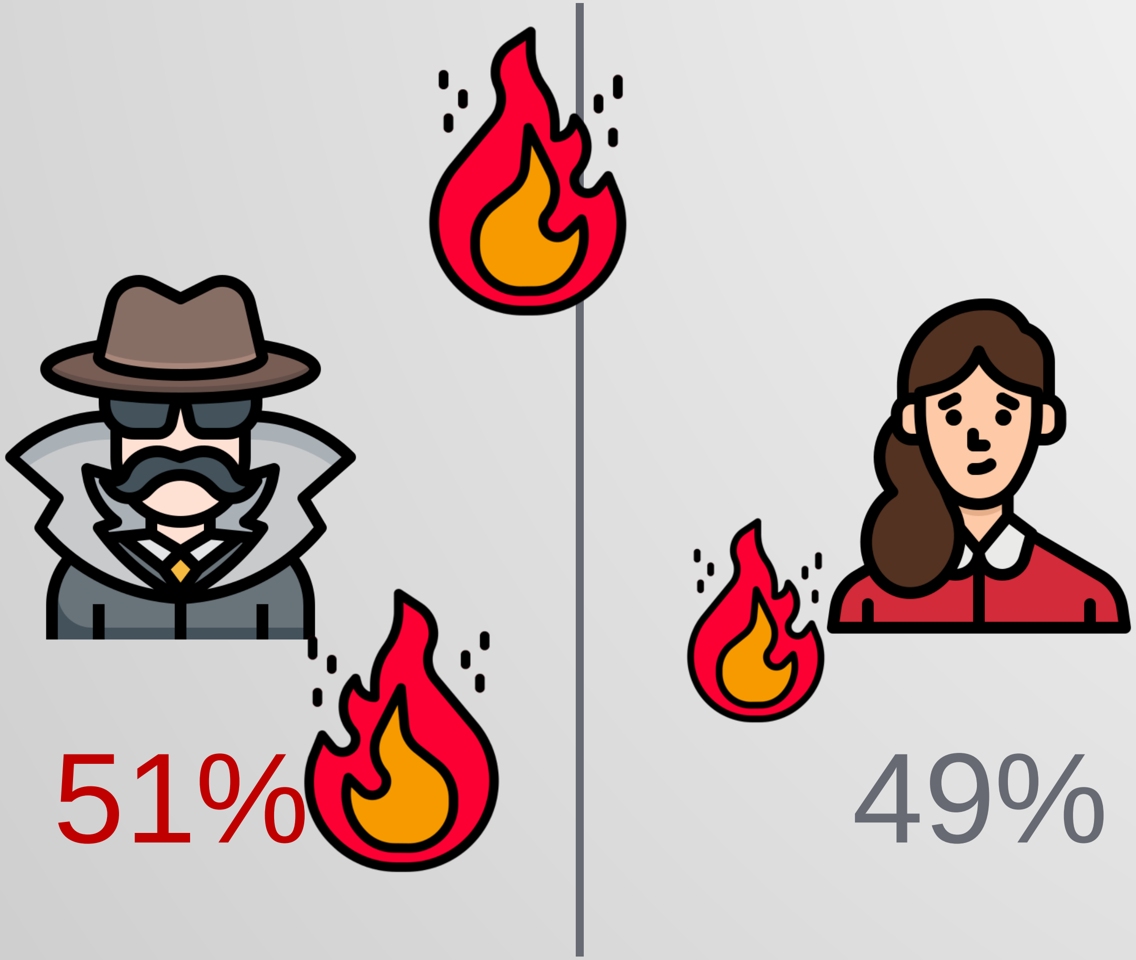
Back to byzantine generals

13%



87%

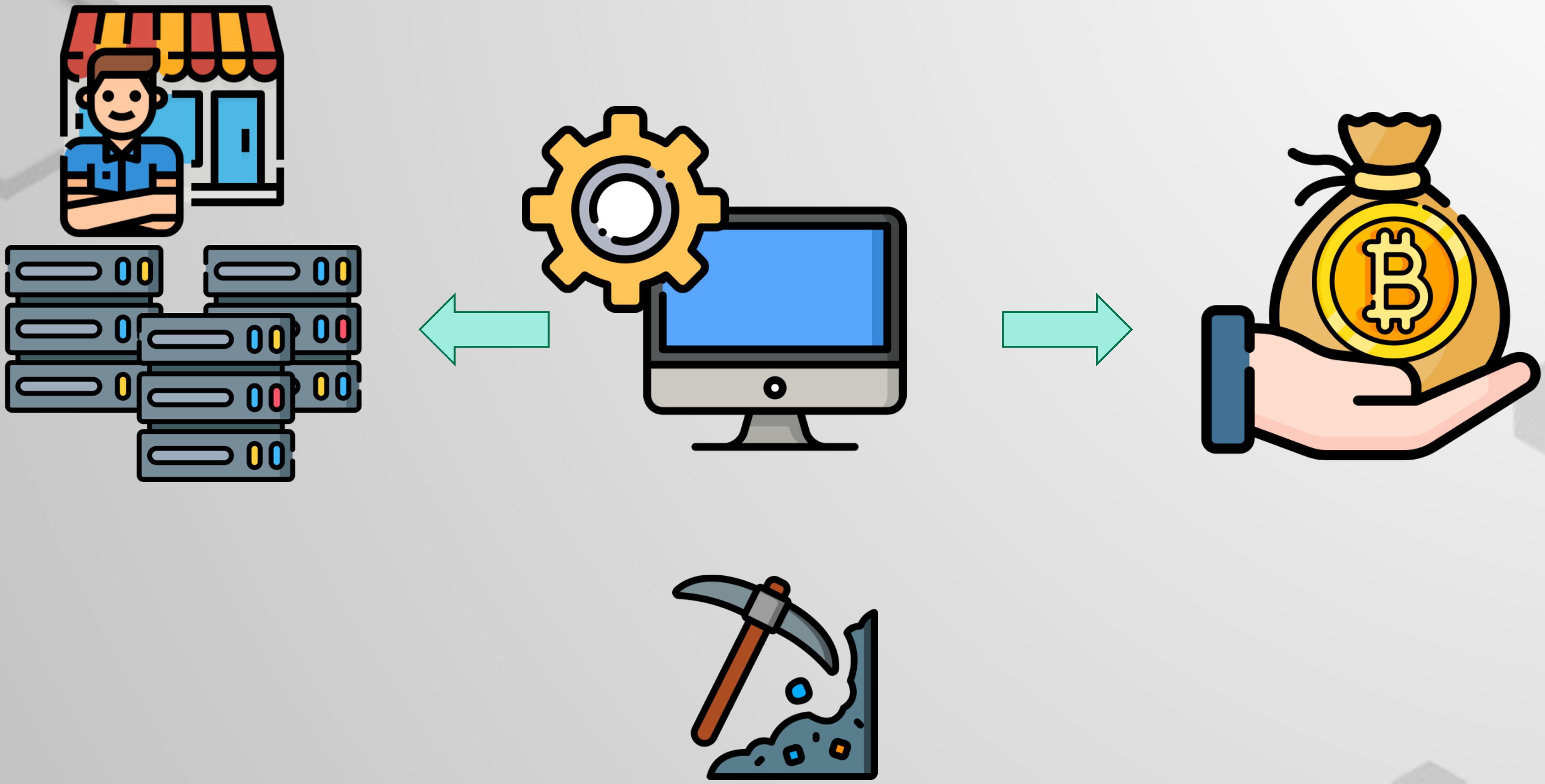
Back to byzantine generals



51%

49%

Motivation to operate the network



Summary

Immutability

Security

Decentralization

Adaptability

Automatization

SIMPLE !

International stakes

Applications

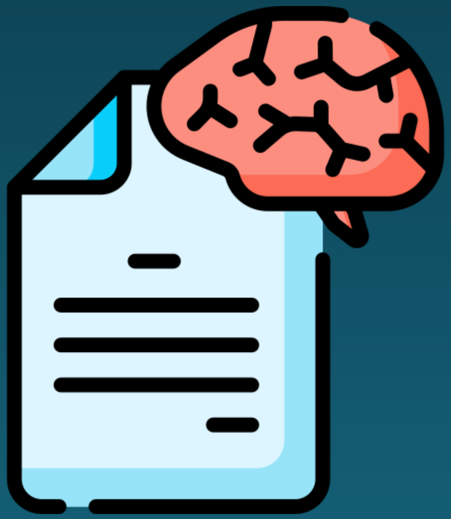
Cryptocurrencies
(Bitcoin, Ethereum)

Medicine

Voting

WEB 3

Applications



Smart Contracts

Examples