Blockchain! General concepts.

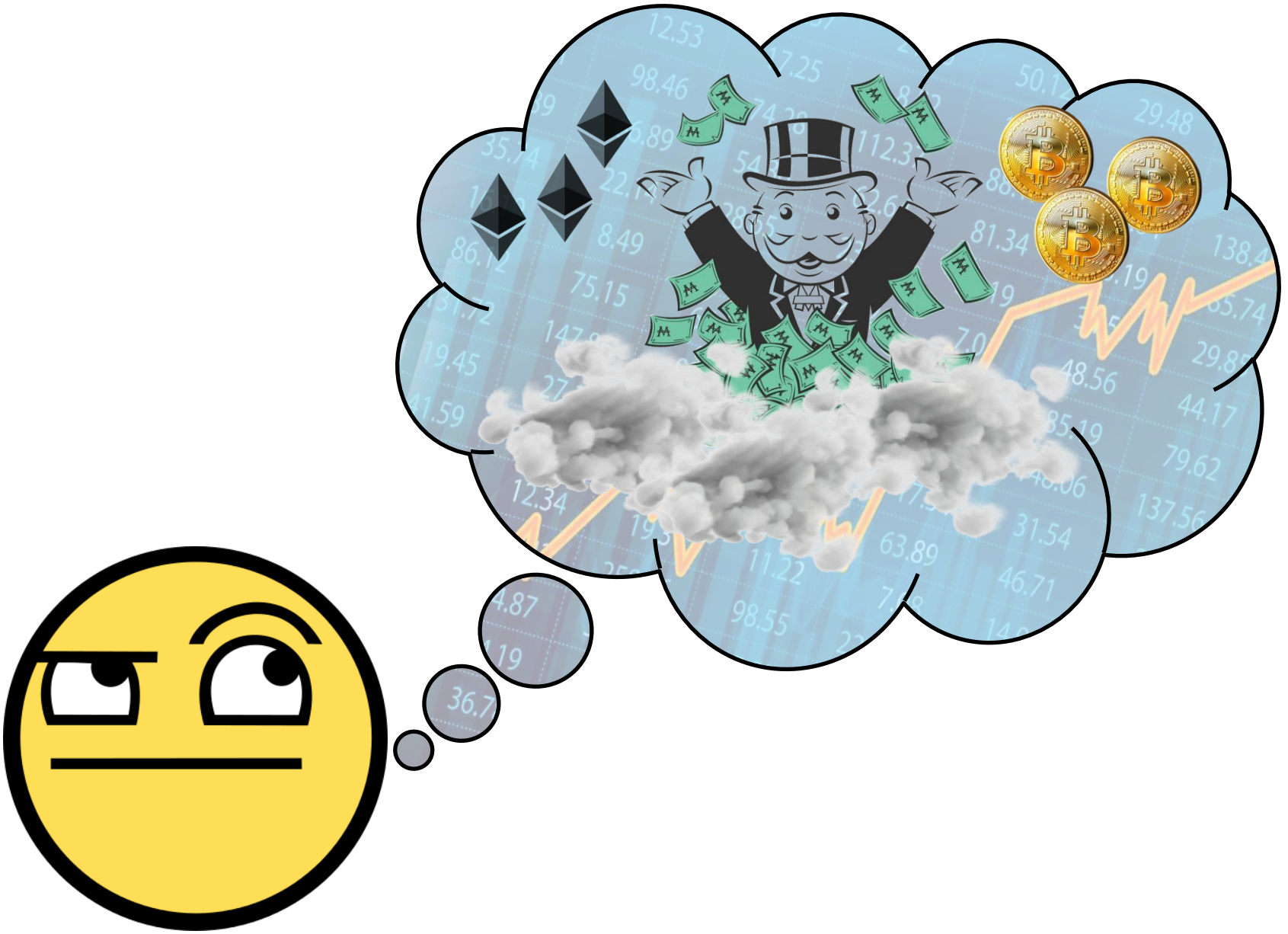
Juan Cano-Benito
Ontology Engineering Group
Universidad Politécnica de Madrid, Spain

jcano@fi.upm.es
@jucanbe

25/09/2019
Madrid, Spain

CC BY SA

Blockchain. What the people thinks



- Basic concepts
- Security
- Contributions
- Smart Contracts
- Applications

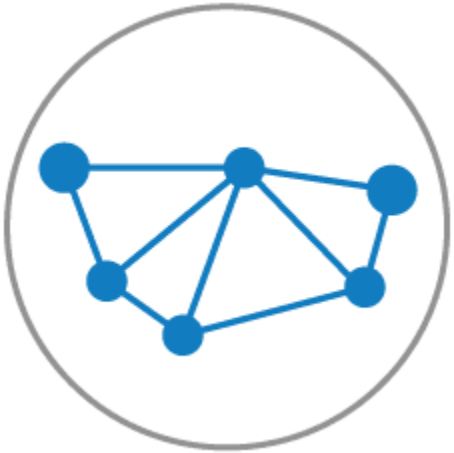
Basic concepts

- Distributed
  - No central entity
- Peer-to-peer network
  - Consensus protocol
- Types
  - Public, consortium, private

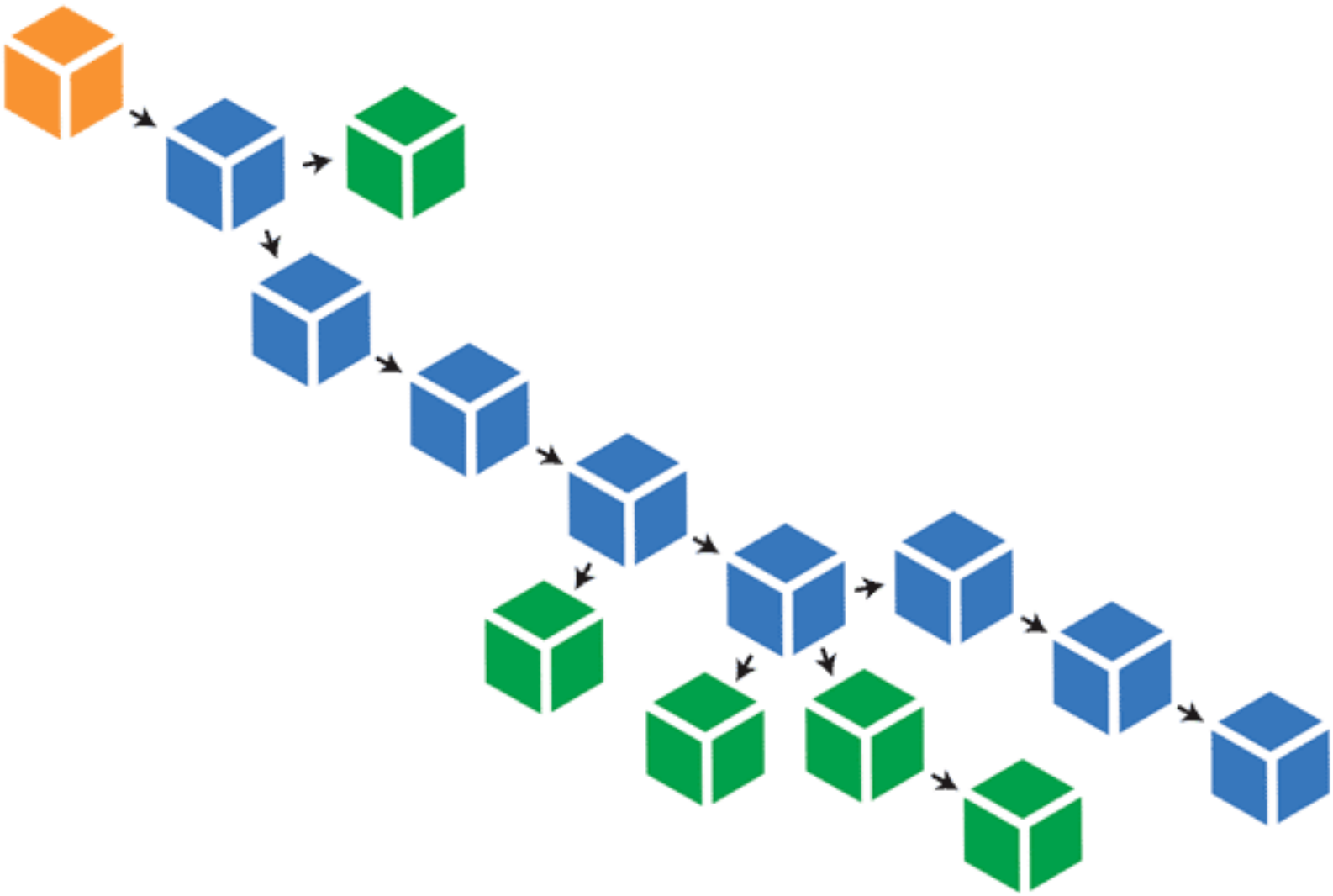
Public

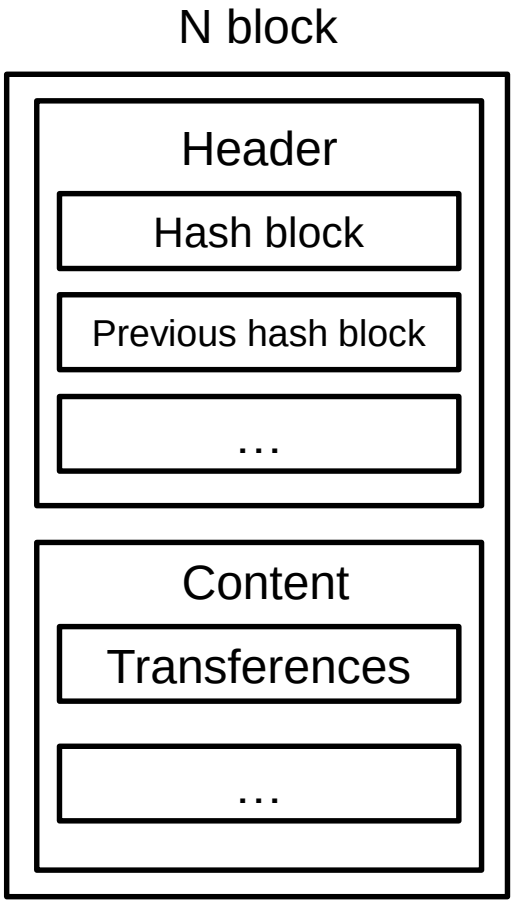
Consortium

Private



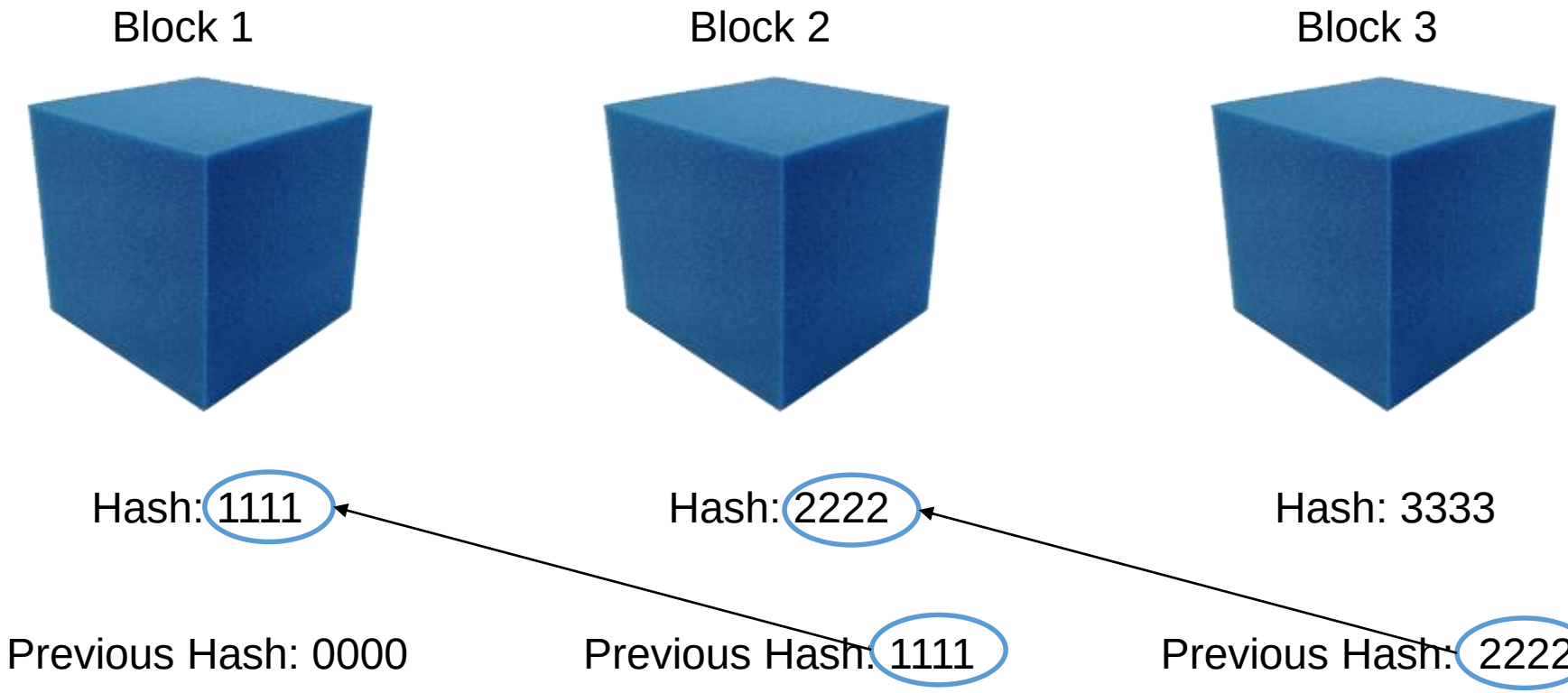
Basic concepts. Blockchain



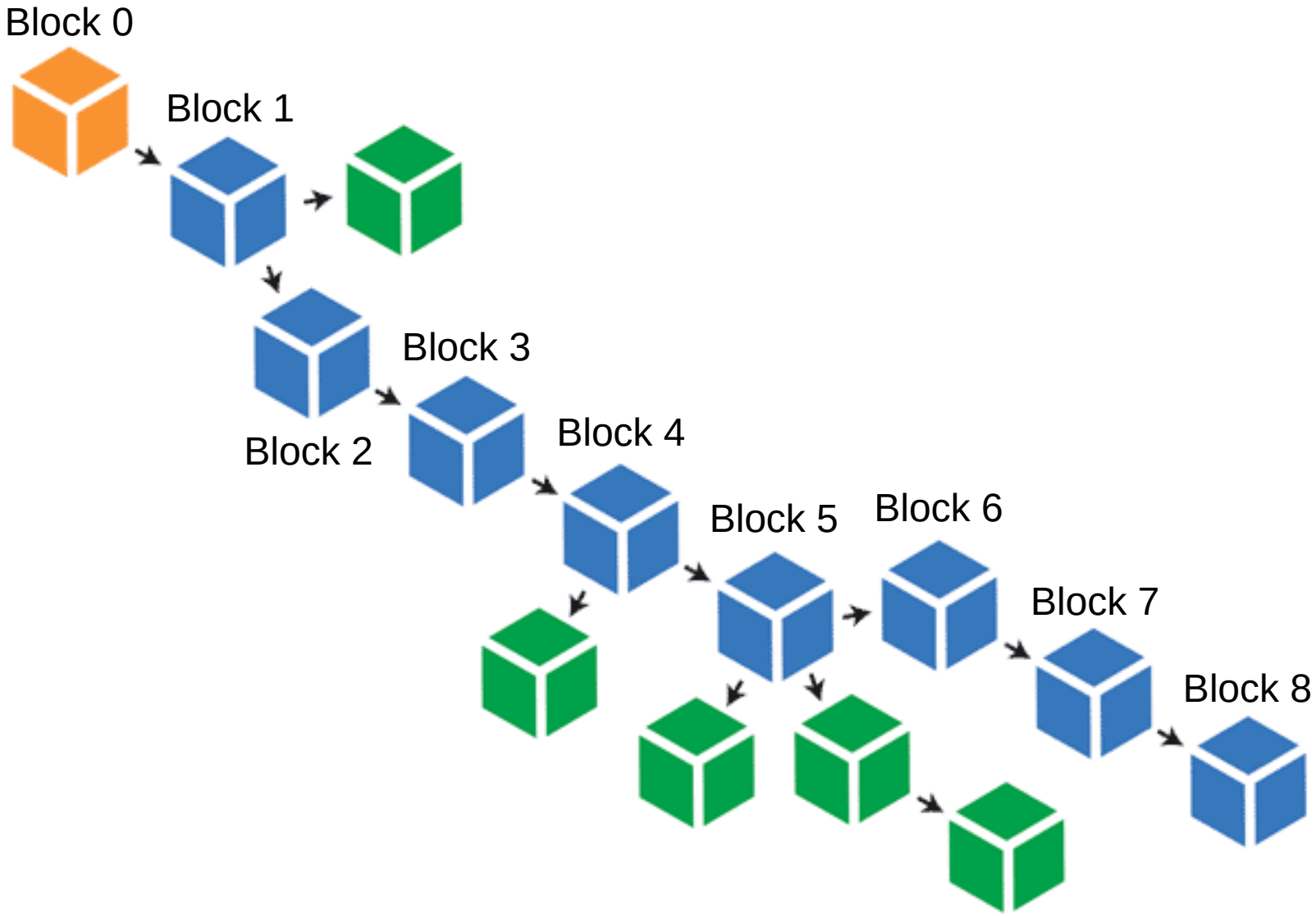


- Block
  - Header
    - Hash, Meta-Data…
  - Content
    - Transferences, other information
    - Storage limitation
- Chain
  - Immutability

Basic concepts. Chain

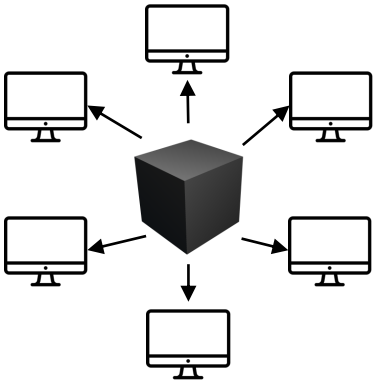


Basic concepts. Blockchain

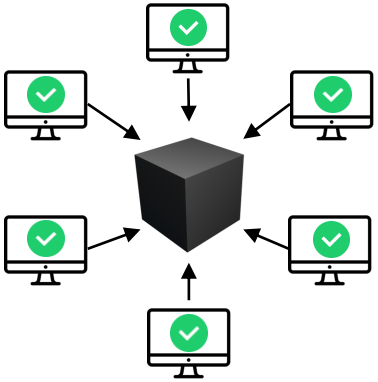


Basic concepts. New blocks.

New block discovered!



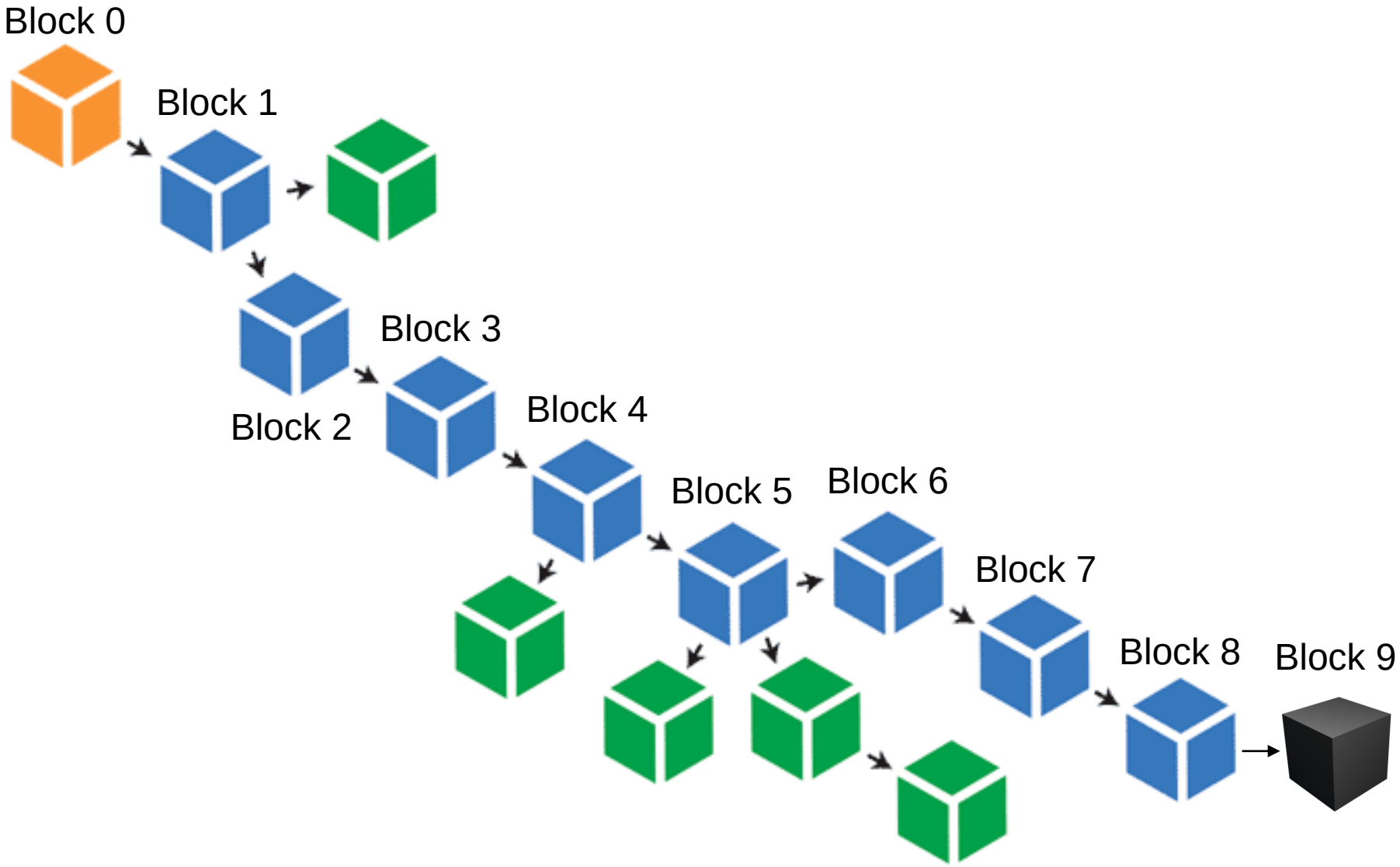
Send the new block to everyone in the network



Each node verifies the new block

The block is added to the blockchain

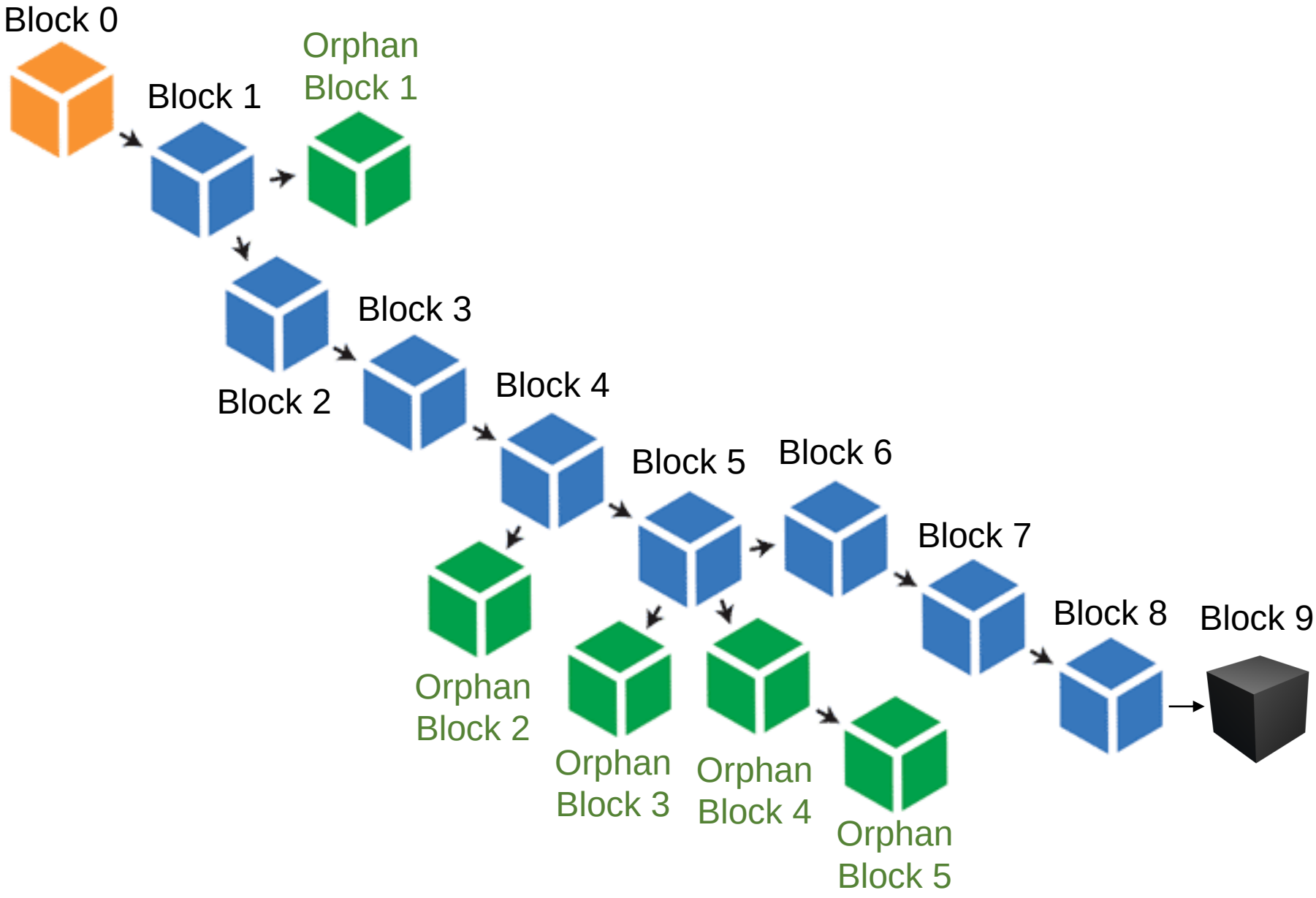
Basic concepts. Blockchain



Basic concepts. Orphan blocks

- Are produced when 2 or more blocks are discovered at almost the same time
- Valid blocks that are not part of the main chain

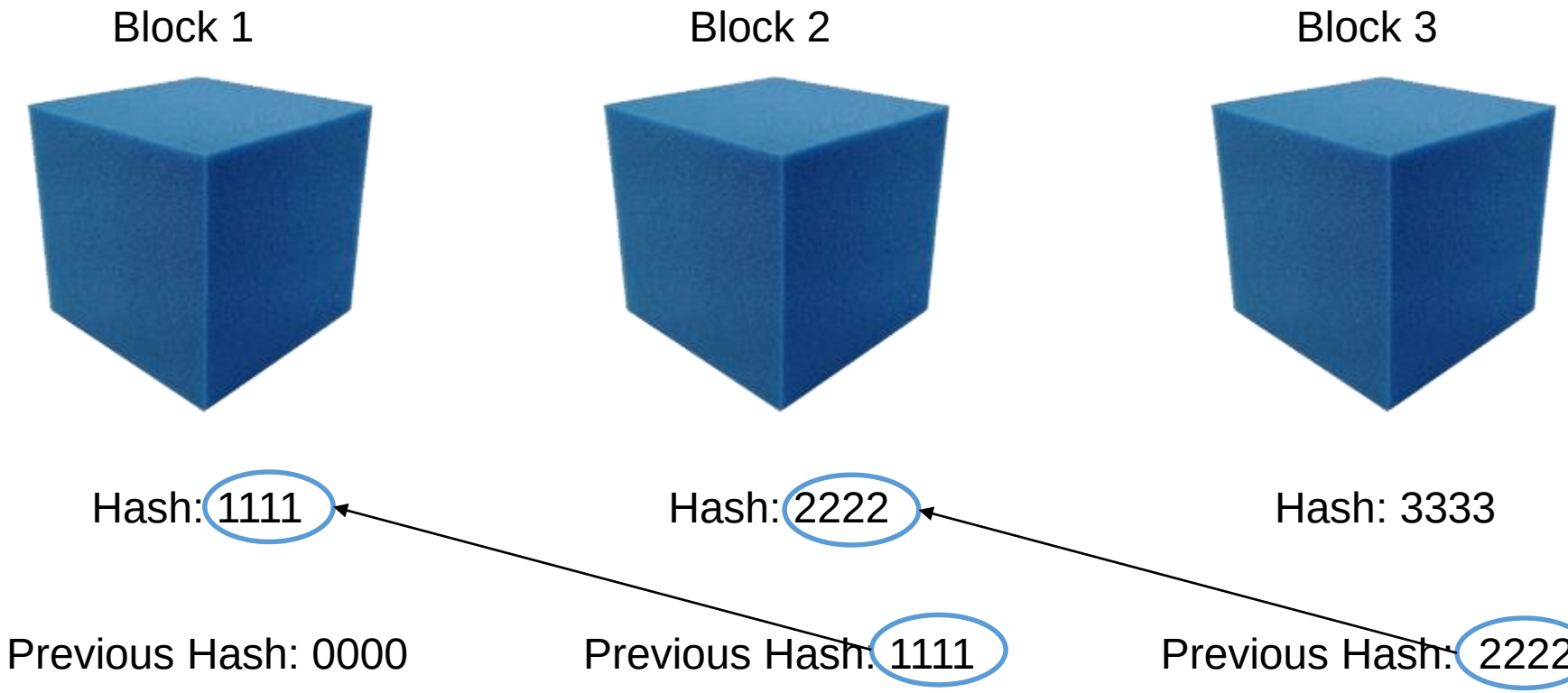
Basic concepts. Blockchain



- Basic concepts
- Security
- Contributions
- Smart Contracts
- Applications

Security

- Blockchain security is due to 3 factors.
  - Hashing
  - Proof-of-Work
  - Distributed


Block 1
Block 2
Block 3
Hash: 1111
Hash: 2222
Hash: 3333
Previous Hash: 0000
Previous Hash: 1111
Previous Hash: 2222

Block 1

Hash: 1111

Previous Hash: 0000

Block 2

Hash: 2 2 BBBB

Previous Hash: 1111

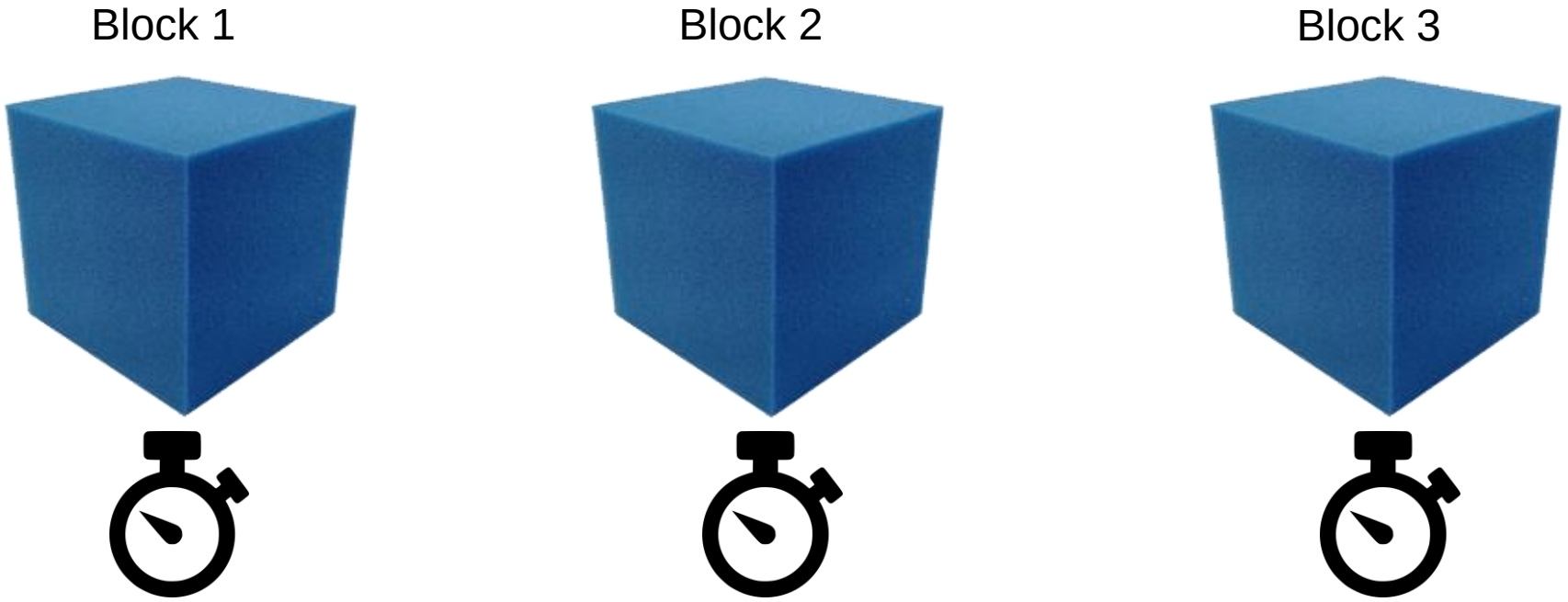
Block 3

Hash: 3333

Previous Hash: 2222

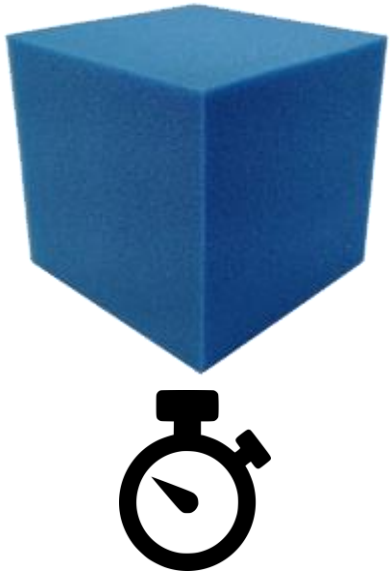
Wait, thats not right!

- Mechanism that slows down the creation of new blocks

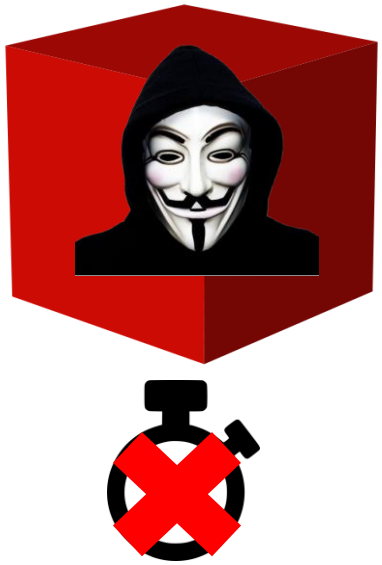


- If someone tamper 1 block, he need to recalculate the proof-of-work for all the following blocks

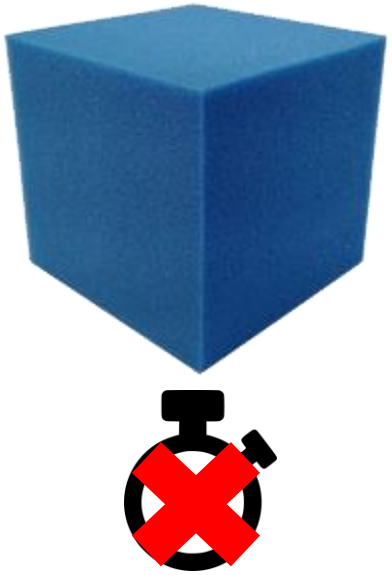
Block 1



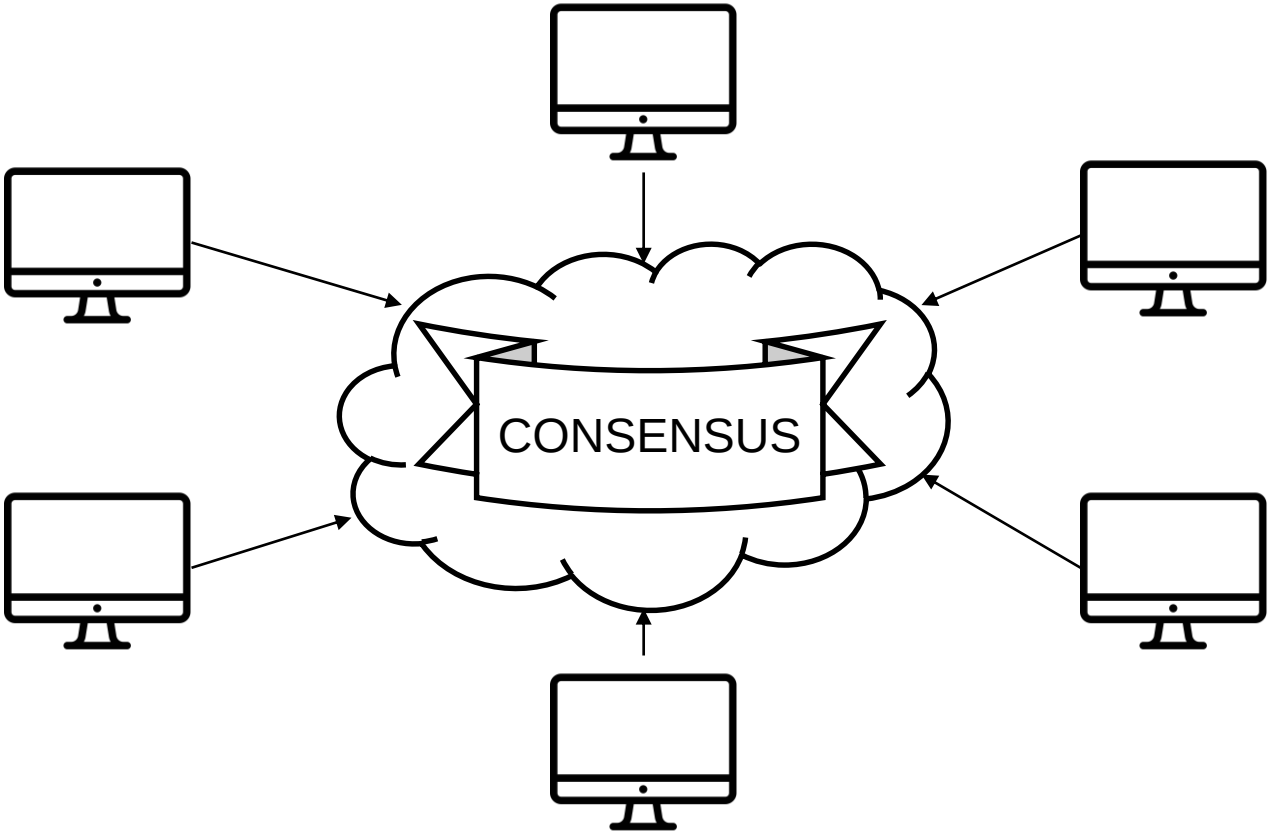
Block 2



Block 3



- The most important characteristic
- All the nodes works in consensus
  - Nodes agree about what blocks are valid and which aren't
  - Modified blocks will be rejected by the rest of the nodes

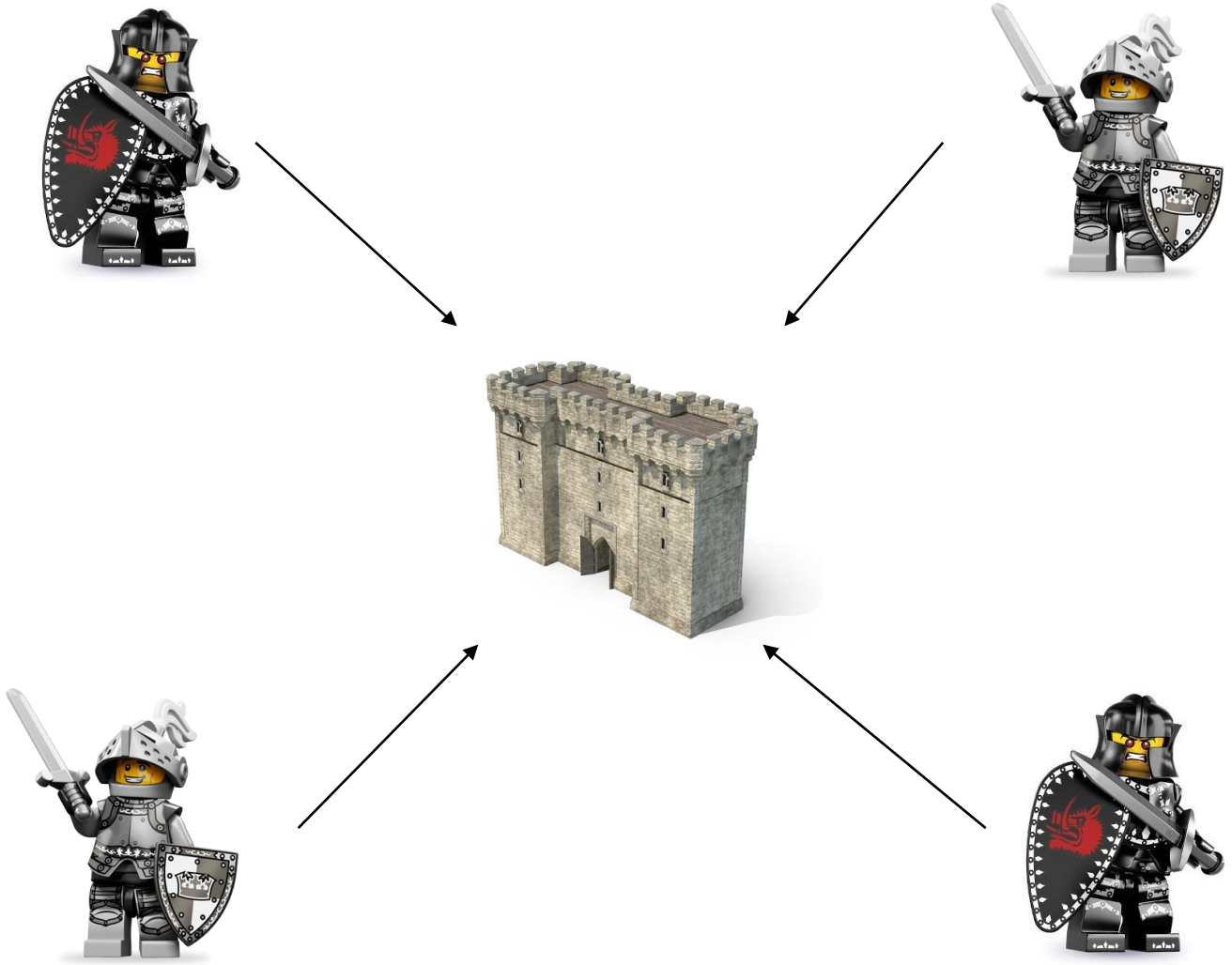


Security. Conclusion

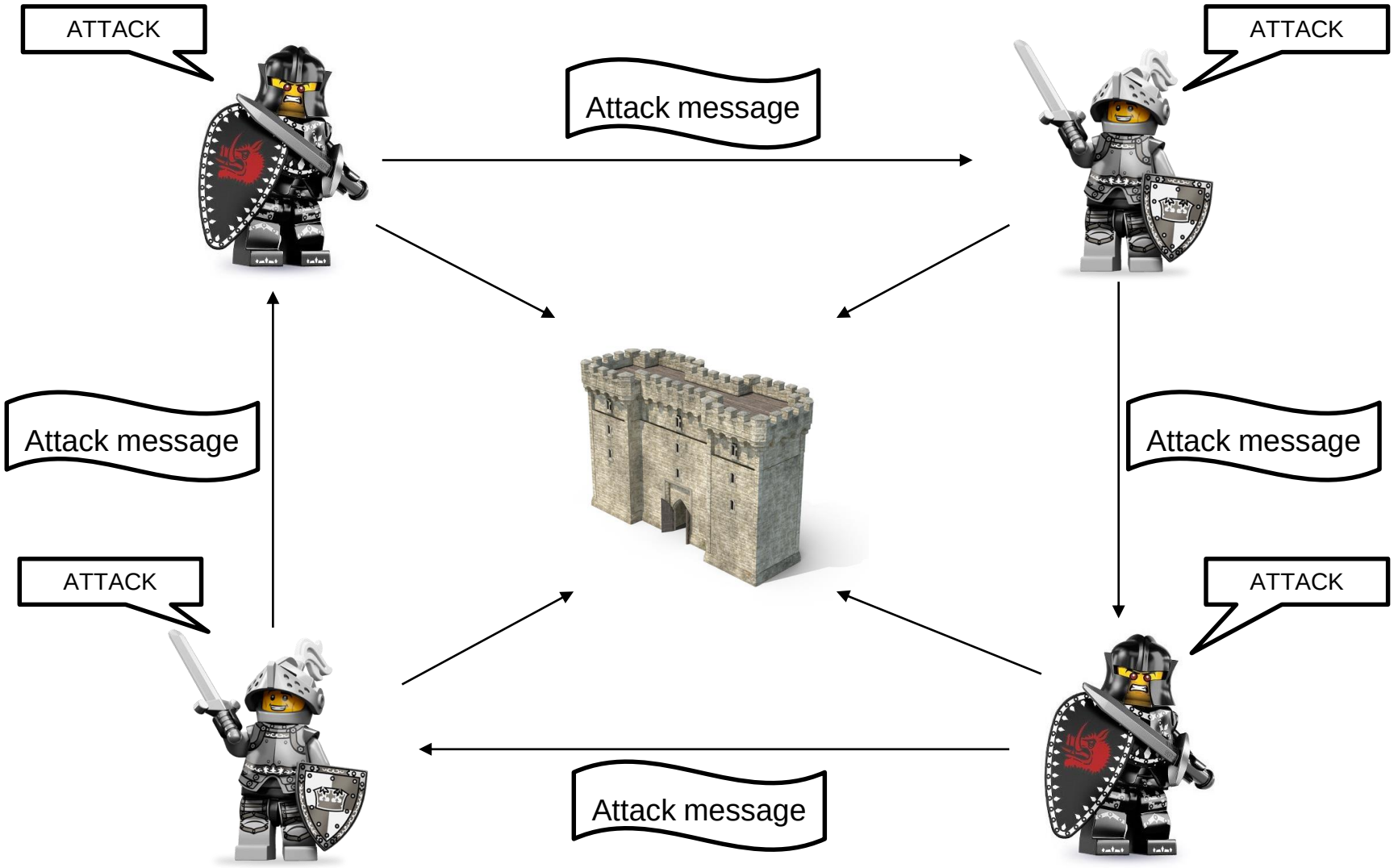
- To modify the blockchain:
  - Have to alterate all the blocks in the chain
  - Redo the proof-of-work
  - Control more than the 50% of the network

- Basic concepts
- Security
- Contributions
- Smart Contracts
- Applications

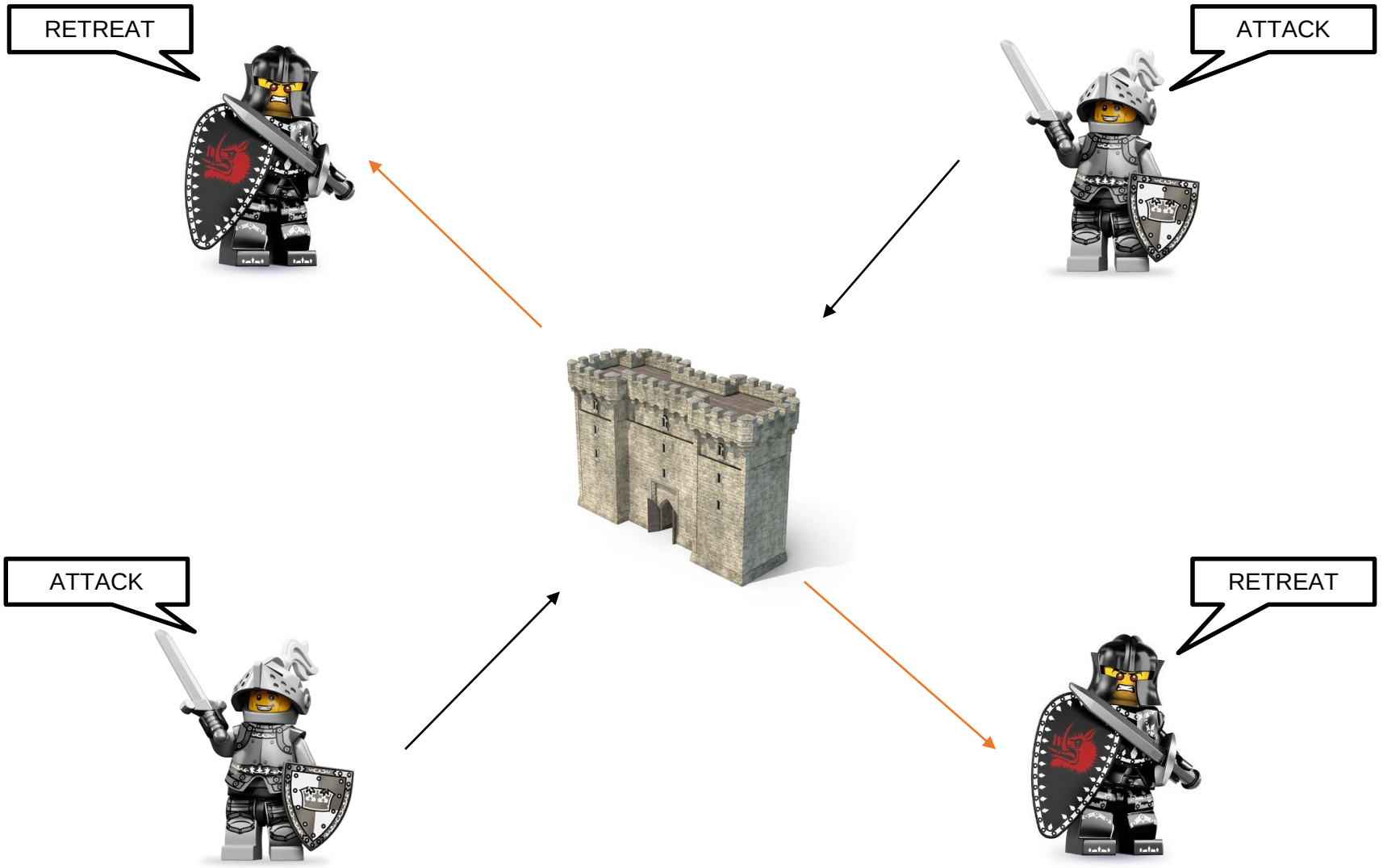
Contributions. Byzantine fault



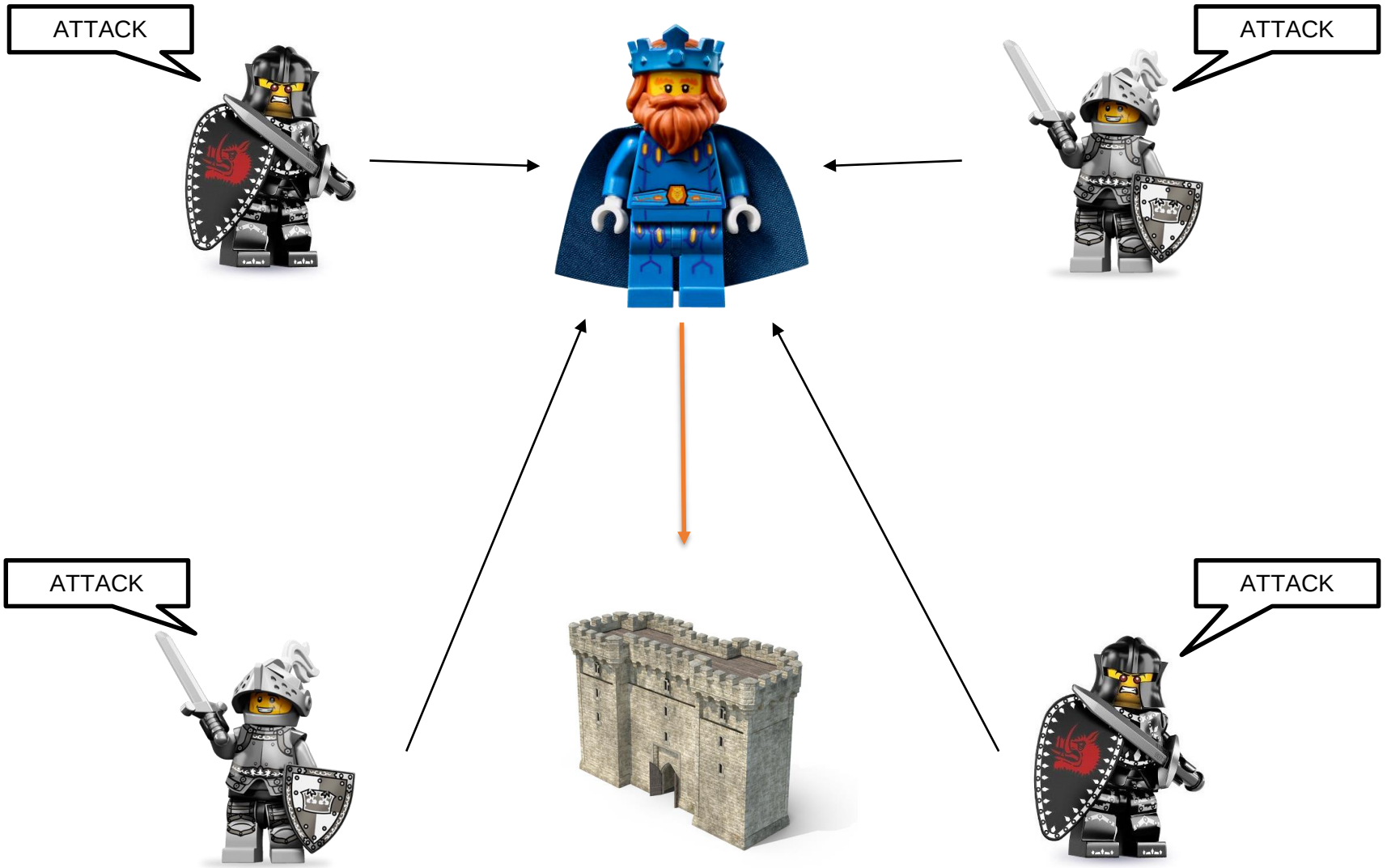
- Problem on the tradicional distributed systems



- Result

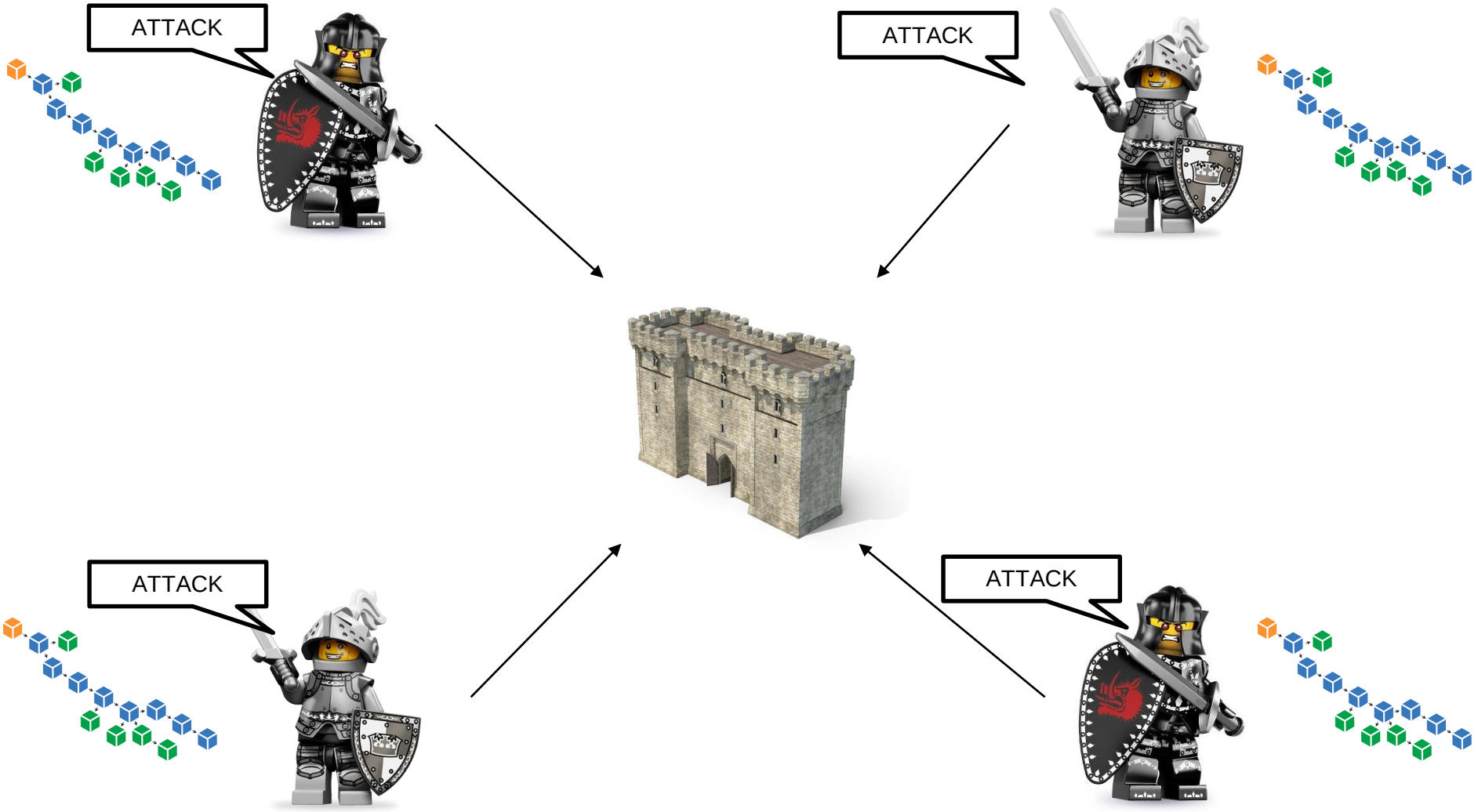


- Central authorities



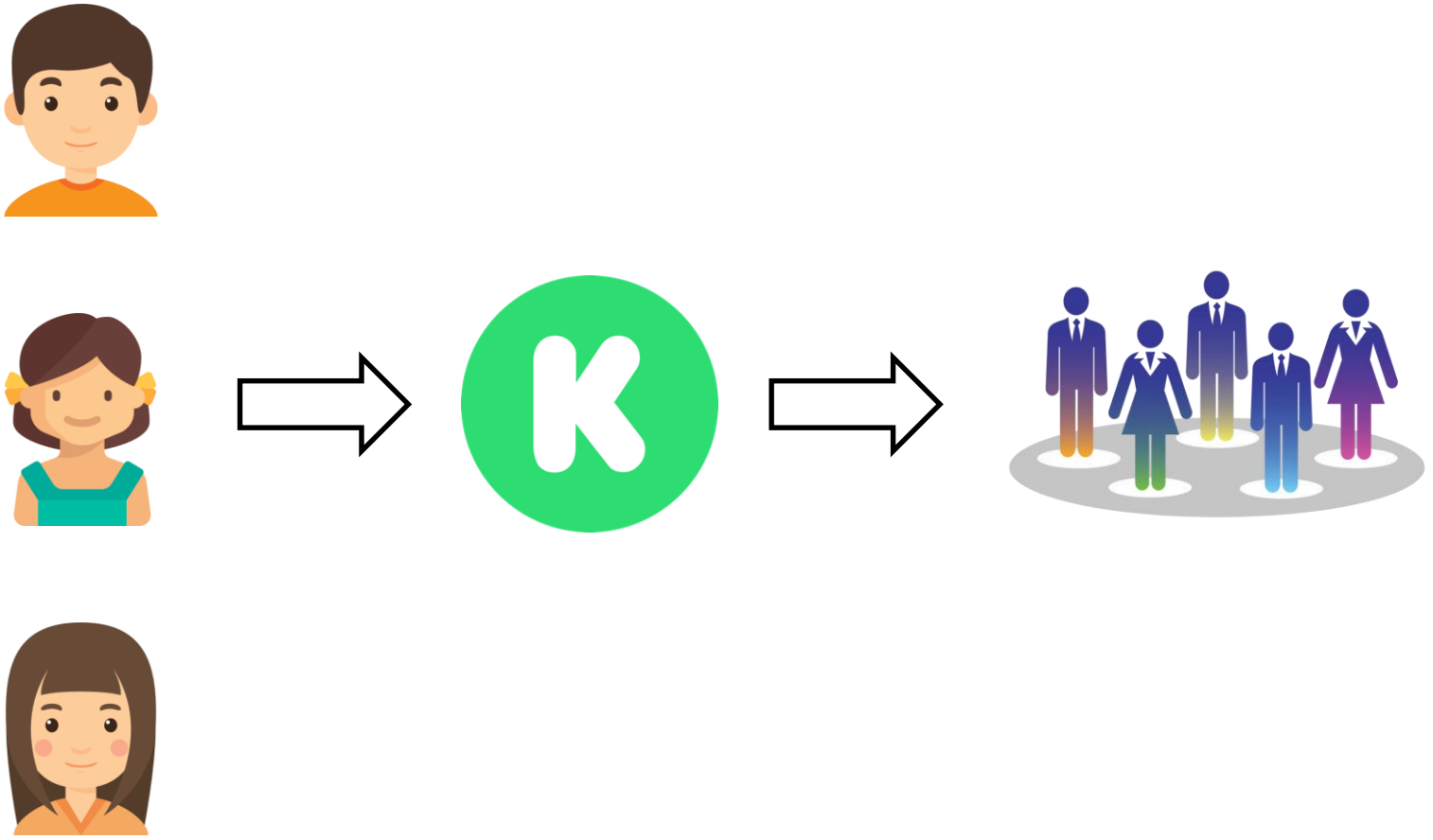
Contributions. Byzantine fault tolerance

- Blockchain. Each general have a copy of the actions of the other generals

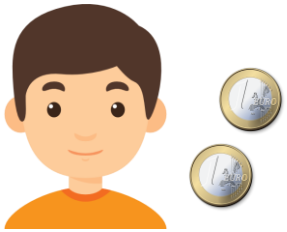


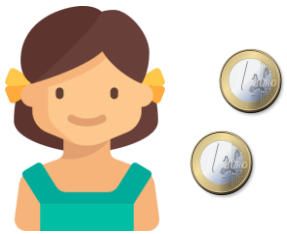
- Basic concepts
- Security
- Contributions
- Smart Contracts
- Applications

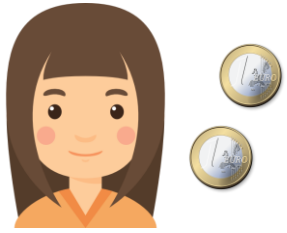
- Trust in a third party



- Similar system without third party







- Project founded!

- Project failed!

Smart Contracts. Properties

- Inherit blockchain properties
  - Inmutability
    - Once a Smart Contract is created, it can never be changed again
  - Distributed
    - The output of the contract is validated by everyone
- The most important blockchain to process Smart Contracts is Ethereum
  - It was created and designed to support Smart Contracts

- Basic concepts
- Security
- Contributions
- Smart Contracts
- Applications

Applications

- Money
- Financial
  - Nasdaq
- Property registration
  - Japan Property Registry
- Digital identity
  - Onename, Keybase, ShoCard…
- Public services
  - Bureaucratic paperwork in Estonia
  - Fight against corruption
- Voting
  - Avoiding election manipulation

Applications

- Music
  - Spotify
- Healthcare
  - Blockchain Rx, First Mover…
- IoT
  - IBM Watson IoT Platform
- Companies
  - Facebook Libra
    - Association with Paypal, Visa, Uber, Spotify, Ebay, Vodafone…
  - IBM
  - Nintendo
    - Videogames rental

- Thank you.