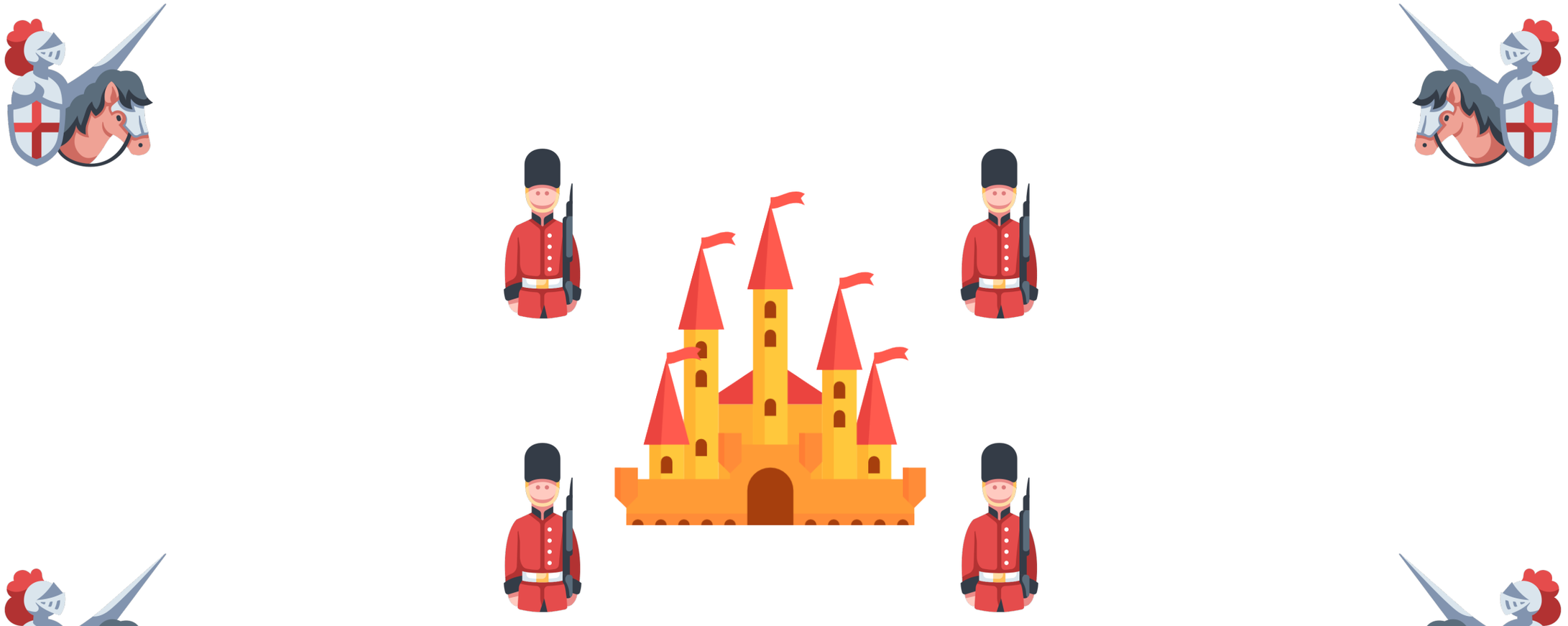
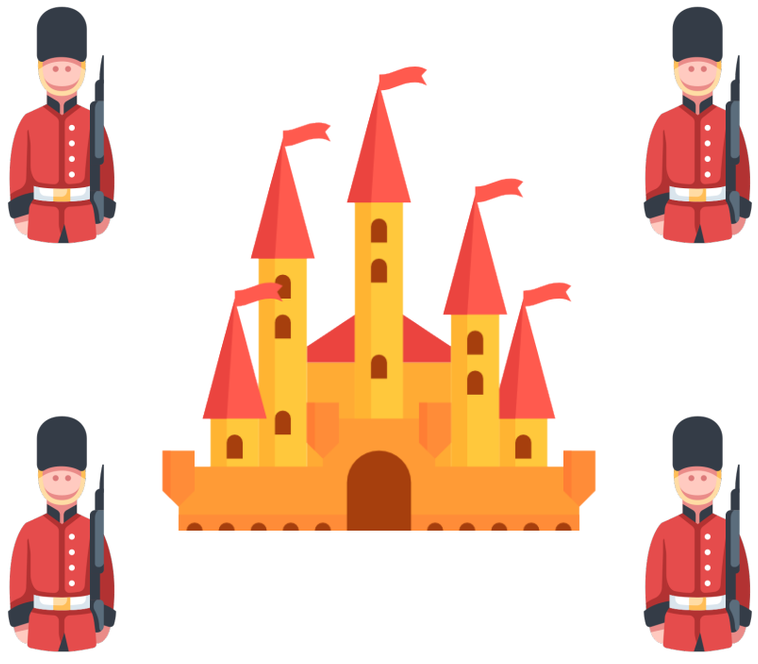
# **Blockchain Background**
Byzantine Generals' Problem

# Byzantine Generals' Problem



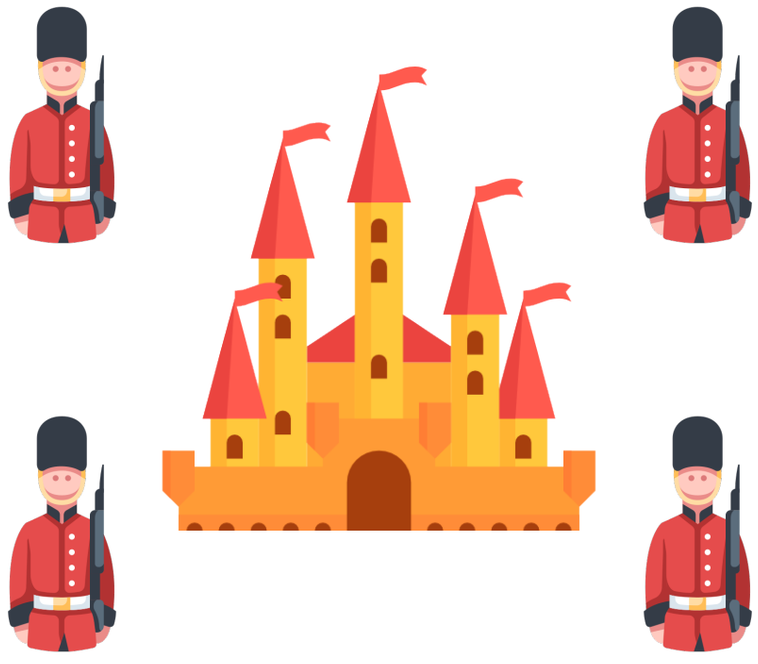
# Byzantine Generals' Problem

Attack?



# Byzantine Generals' Problem

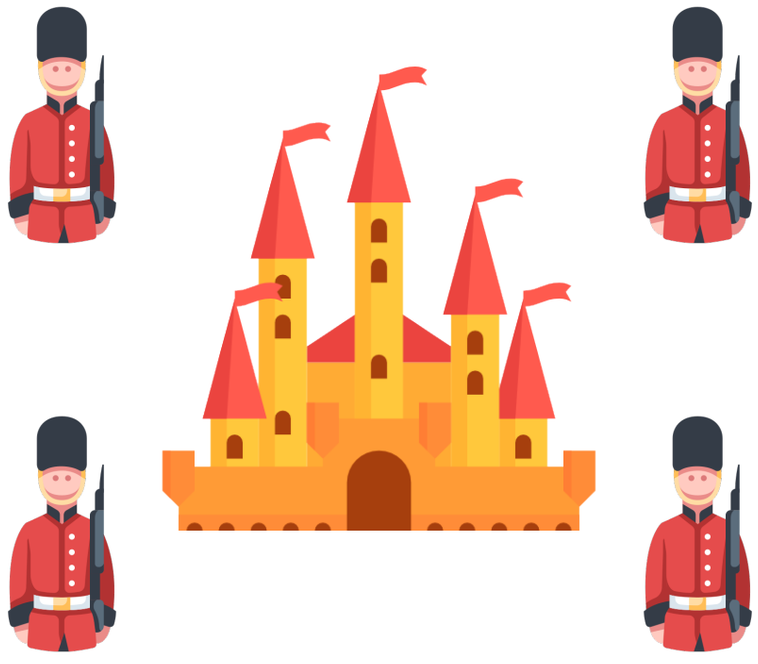
Attack?



Retreat?

# Byzantine Generals' Problem

Attack?

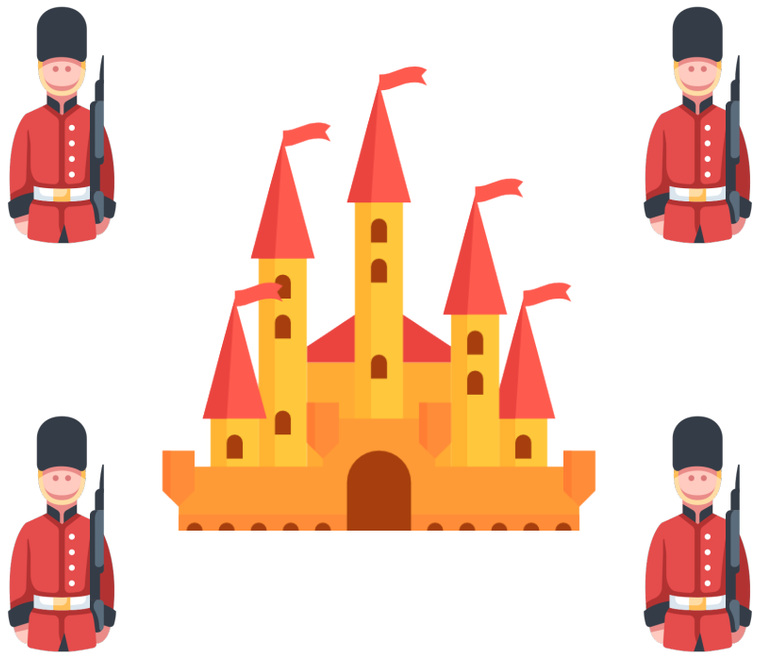


Attack?

Retreat?

# Byzantine Generals' Problem

Attack?



Attack?

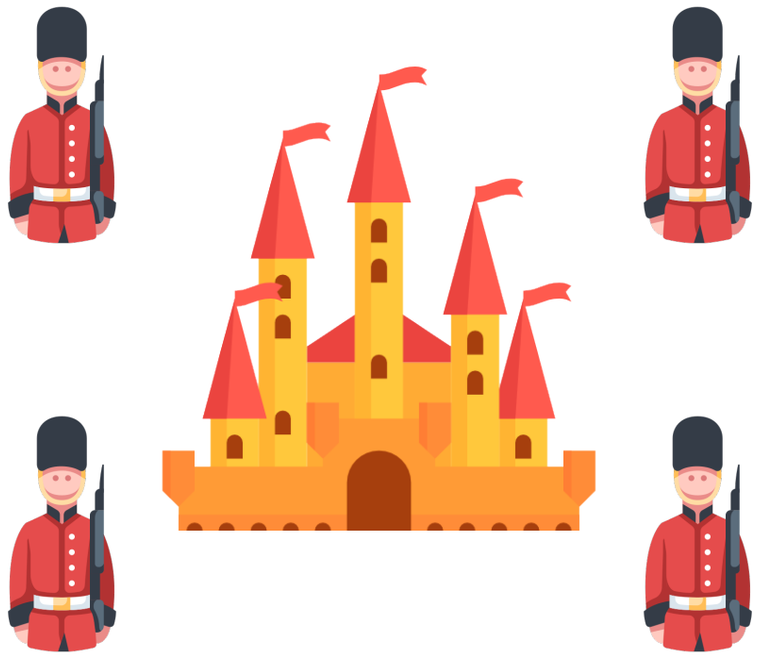
Retreat?

Surrender?

# Byzantine Generals' Problem

- Everyone has to know X
- Everyone knows that everyone knows X
- Everyone knows that everyone knows that everyone knows X

Attack?



Attack?

Retreat?

Surrender?

# Byzantine Generals' Problem

Who does this coin belong to?

Who does this coin belong to?

Who does this coin belong to?

Who does this coin belong to?

# Byzantine Generals' Problem

Who does this coin belong to?

Far away

Who does this coin belong to?

Who does this coin belong to?

Who does this coin belong to?

# Byzantine Generals' Problem

Far away

Who does this coin belong to?

Who does this coin belong to?

How to agree, before taking an action?

Who does this coin belong to?

Who does this coin belong to?

# (Centralised) Digital Payment Systems

Alice

The coin belongs to Alice.

Bob

- Examples
  - Pepper Micropayments [Rivest]
  - ECash [David Chaum] (privacy preserving)

# (Decentralised) Digital Payment Systems

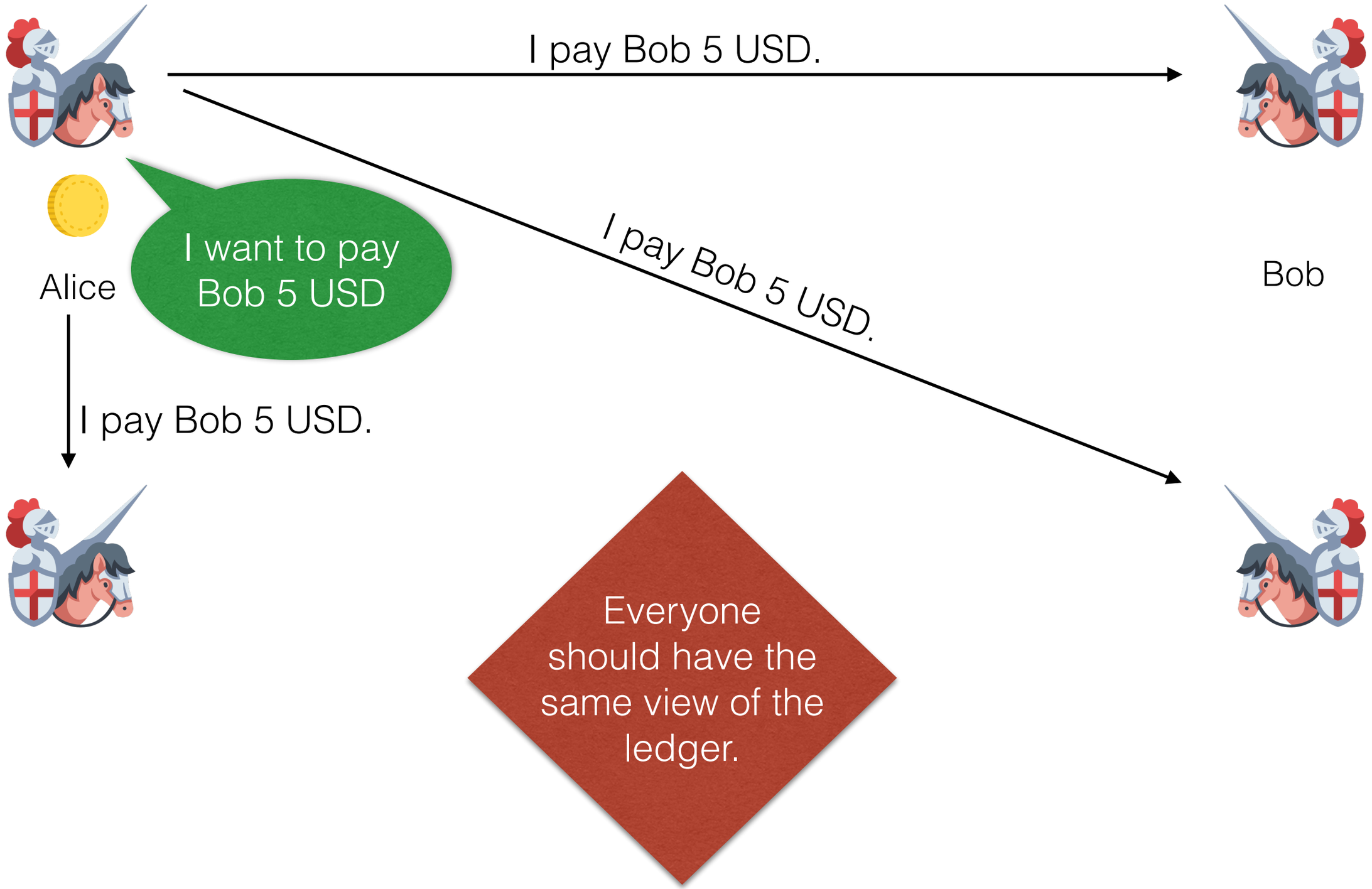
The coin belongs to Alice.

The coin belongs to Alice.

The coin belongs to Alice.

The coin belongs to Bob.

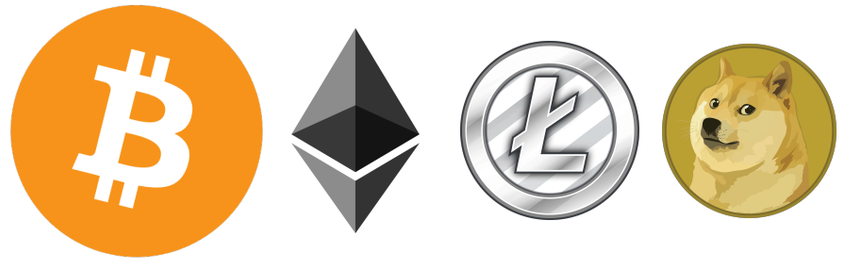
# (Decentralised) Digital Payment Systems



# Blockchain != Blockchain

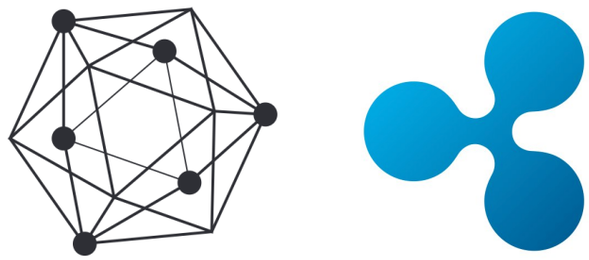
## Open and Decentralised Blockchains

- Ethereum
- Bitcoin



## Permission-based Blockchains

- Hyperledger
- Ripple
- Stellar



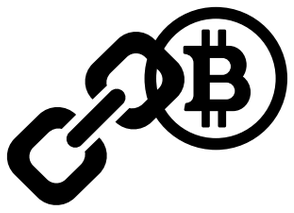
# Bitcoin

- First introduced in 2009
  - Pseudonym Satoshi Nakamoto

- Peer-to-peer decentralised currency

- No trusted third parties (???)

- Blockchain: distributed DB
  - Transactions
  - Blocks



# Bitcoin

- First introc
  - Pseudor
- Peer-to-pe
- No trusted
- Blockchai
  - Transac
  - Blocks