Get a Glimpse of the Popular Fin-tech

BLOCKCHAIN

Yu-Chia Huang
4/27/2021

OUTLINE

- Introduction
- The Origin: The Byzantine General’s Problem
- Byzantine Fault Tolerance Algorithm
- Implementation: Bitcoin
- Reference

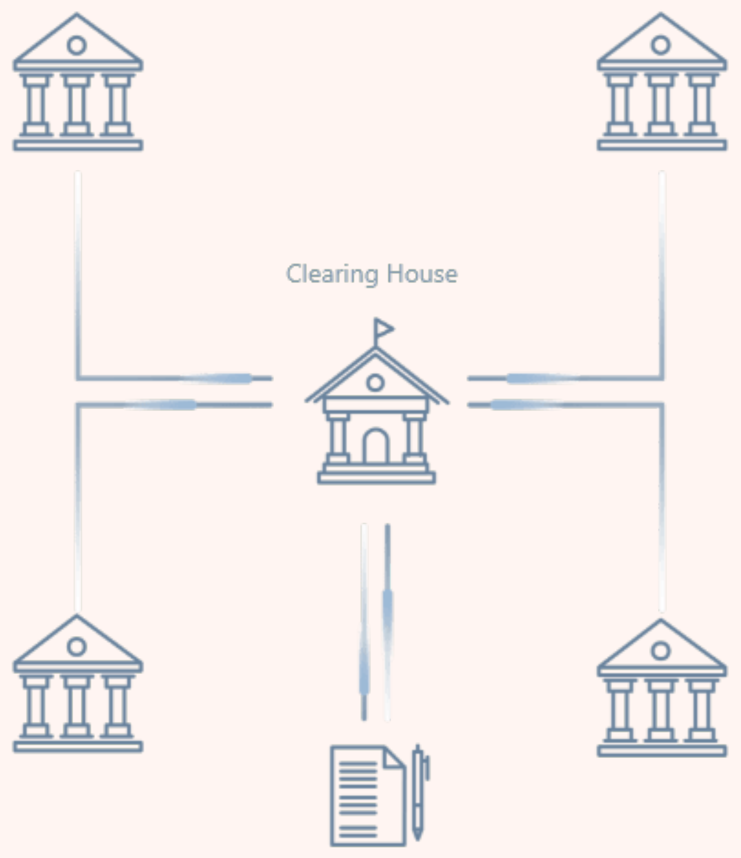
INTRODUCTION

What is blockchain technology?

- **Blockchain defined on IBM’s website:**
  - A shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network.
  - An *asset* can be tangible or intangible. Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved.

KEY ELEMENTS

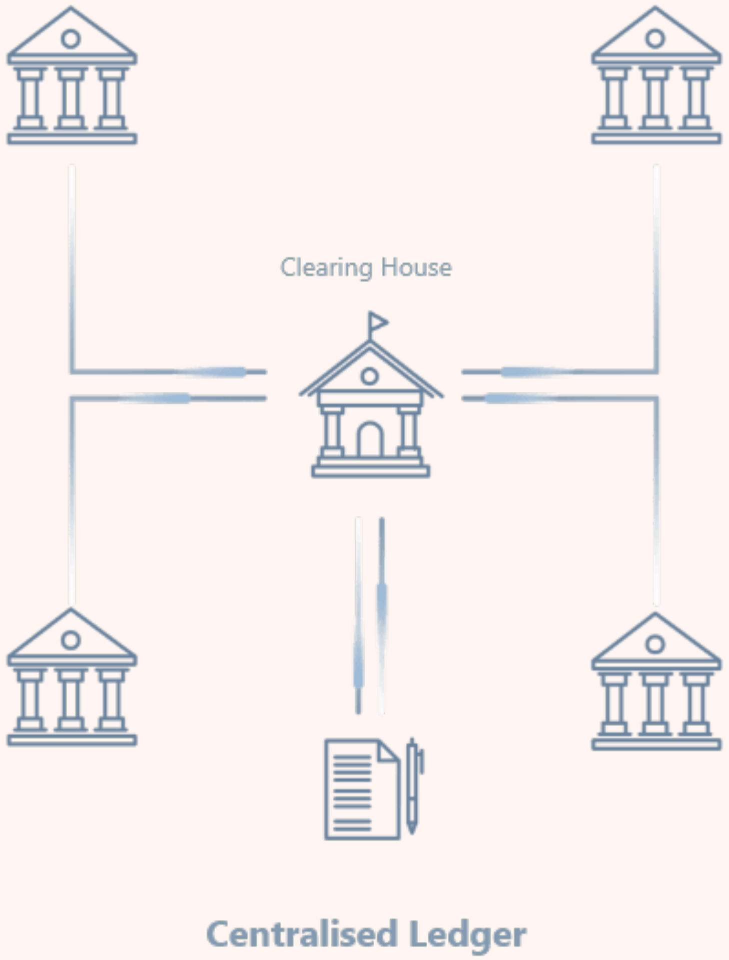
- Distributed ledger technology (DLT)
  - Decentralized and distributed
- Immutable records
- Smart contracts



Centralised Ledger

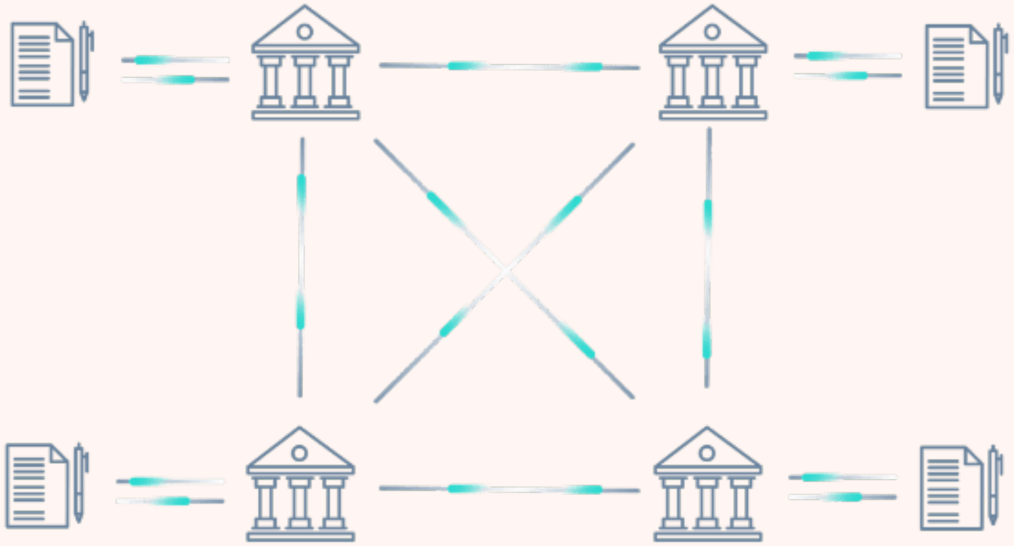
KEY ELEMENTS

- **Distributed ledger technology (DLT)**
  - **Decentralized and distributed**
- **Immutable records**
- **Smart contracts**



KEY ELEMENTS

- Distributed ledger technology (DLT)
  - Decentralized and distributed
- Immutable records
- Smart contracts



Decentralised Ledger

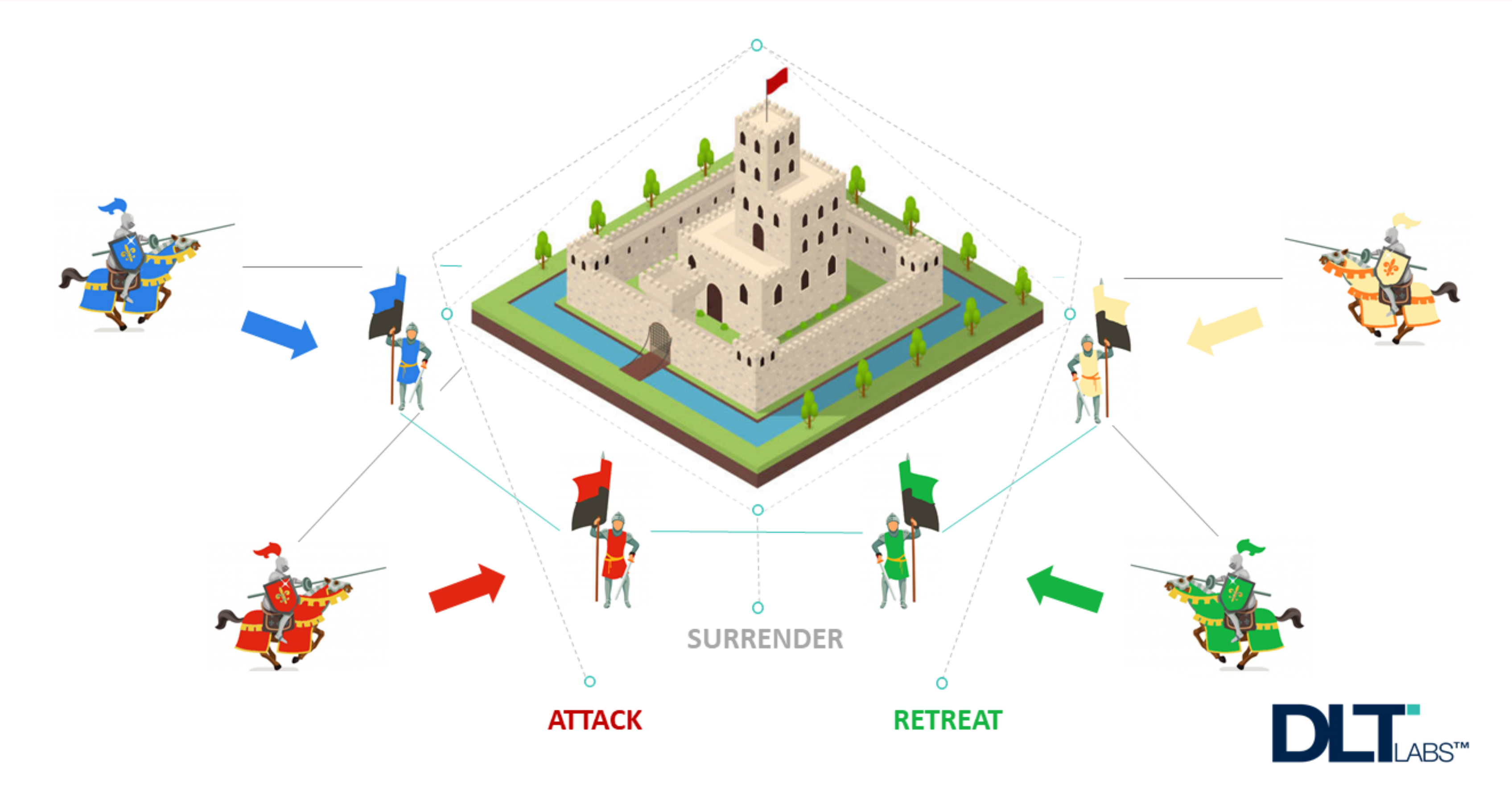
KEY ELEMENTS

- Distributed ledger technology (DLT)
  - Decentralized and distributed
- Immutable records
- Smart contracts

THE ORIGIN:
THE BYZANTINE GENERALS' PROBLEM

1982, LAMPORT, LESLIE, ROBERT SHOSTAK, and MARSHALL PEASE —

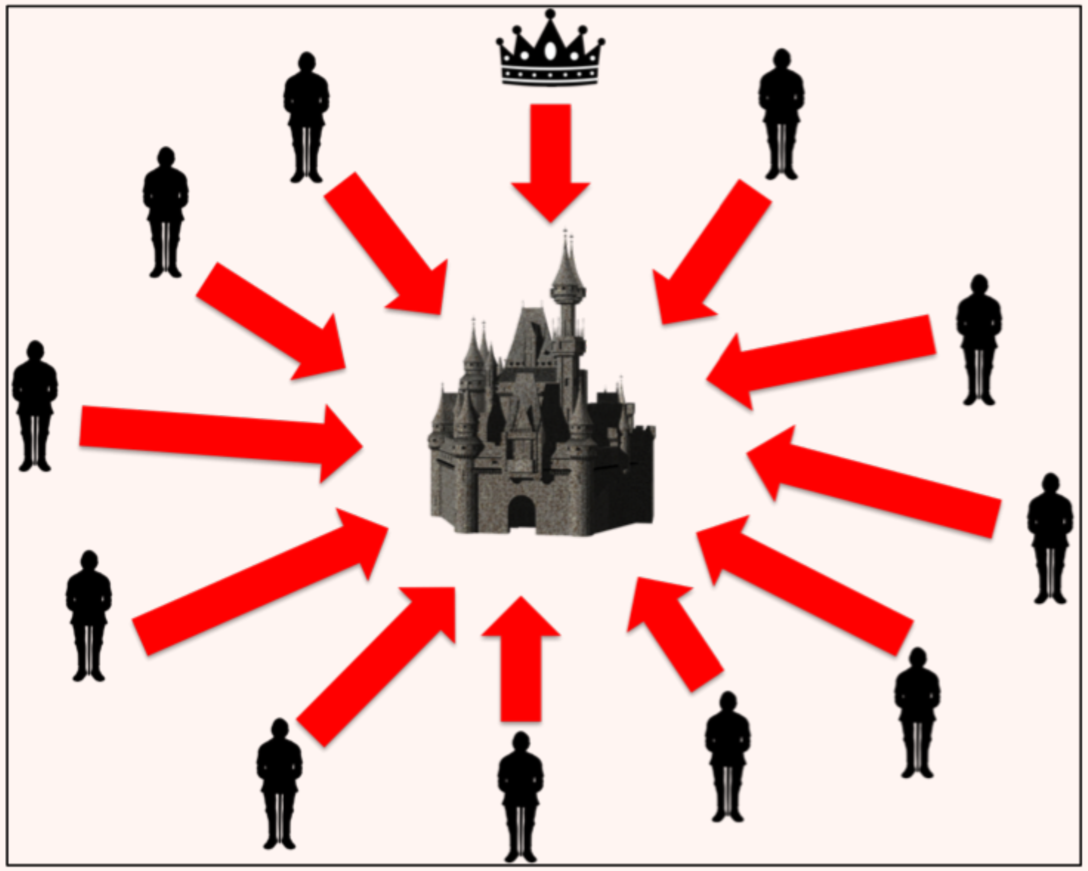
The Byzantine Generals' Problem.



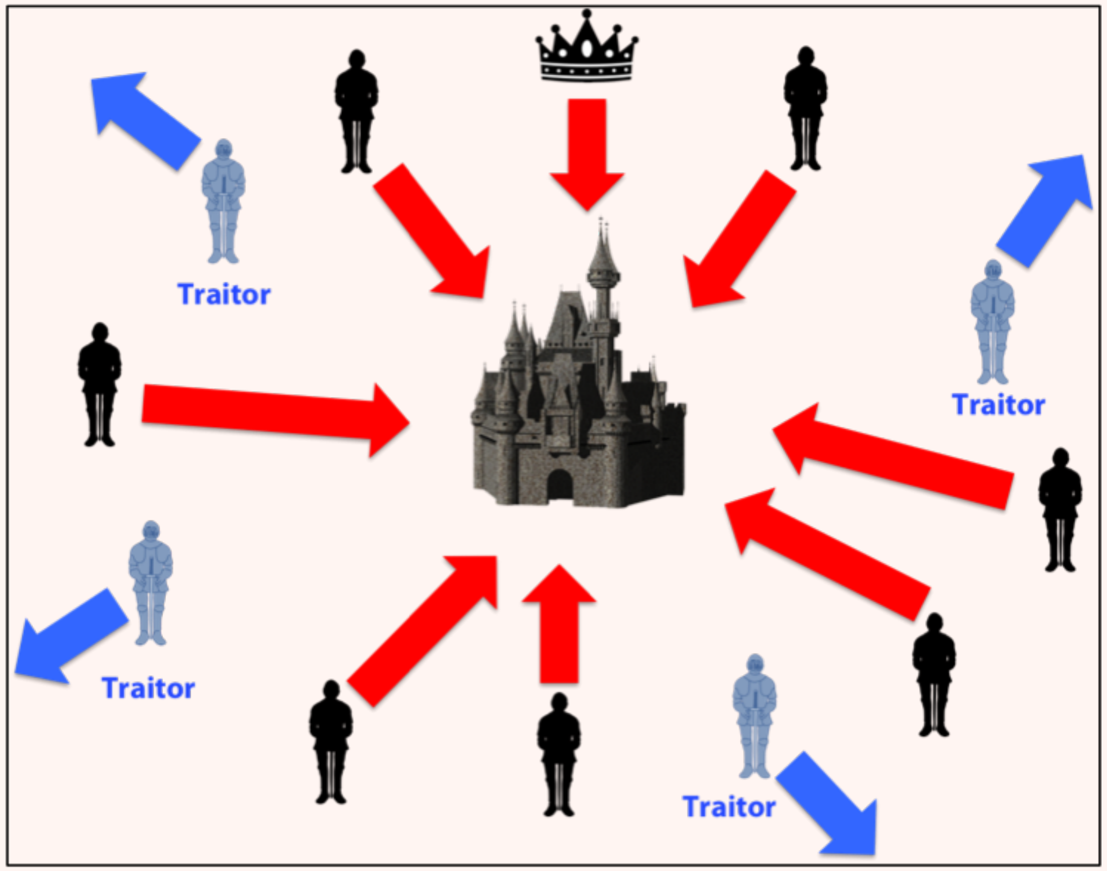
THE BYZANTINE GENERALS' PROBLEM

- We imagine that several divisions of the Byzantine army are camped outside an enemy city, each division commanded by its own general.
- The generals can communicate with one another only by messenger. After observing the enemy, they must decide upon a common plan of action. Assuming that they will succeed only if at least 1/2 of the army attack.
- However, some of the generals may be traitors, trying to prevent the loyal generals from reaching agreement.

THE BYZANTINE GENERALS' PROBLEM



Coordinated Attack Leading to Victory



Uncoordinated Attack Leading to Defeat

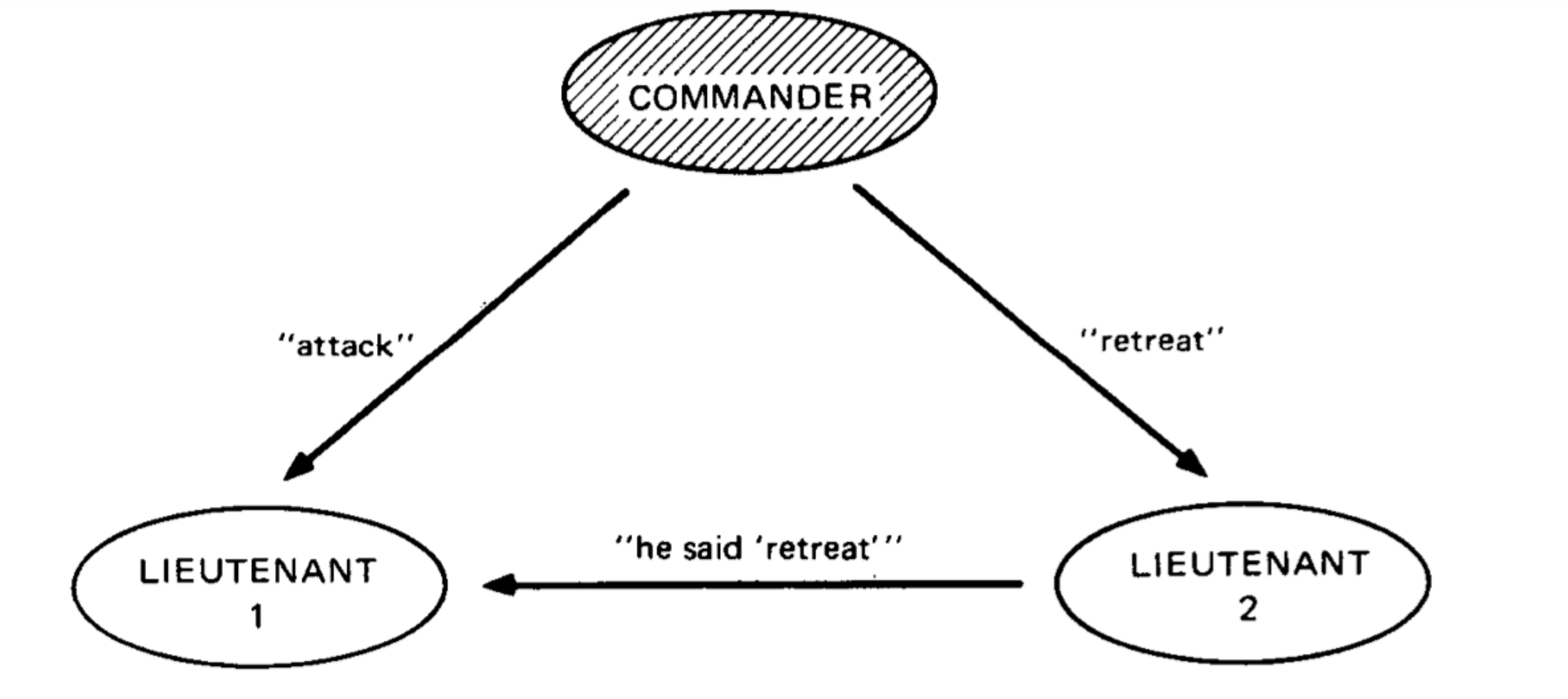
ALGORITHM’S GOALS

- All loyal generals decide upon the same plan of action
- A small number of traitors cannot cause the loyal generals to adopt a bad plan.

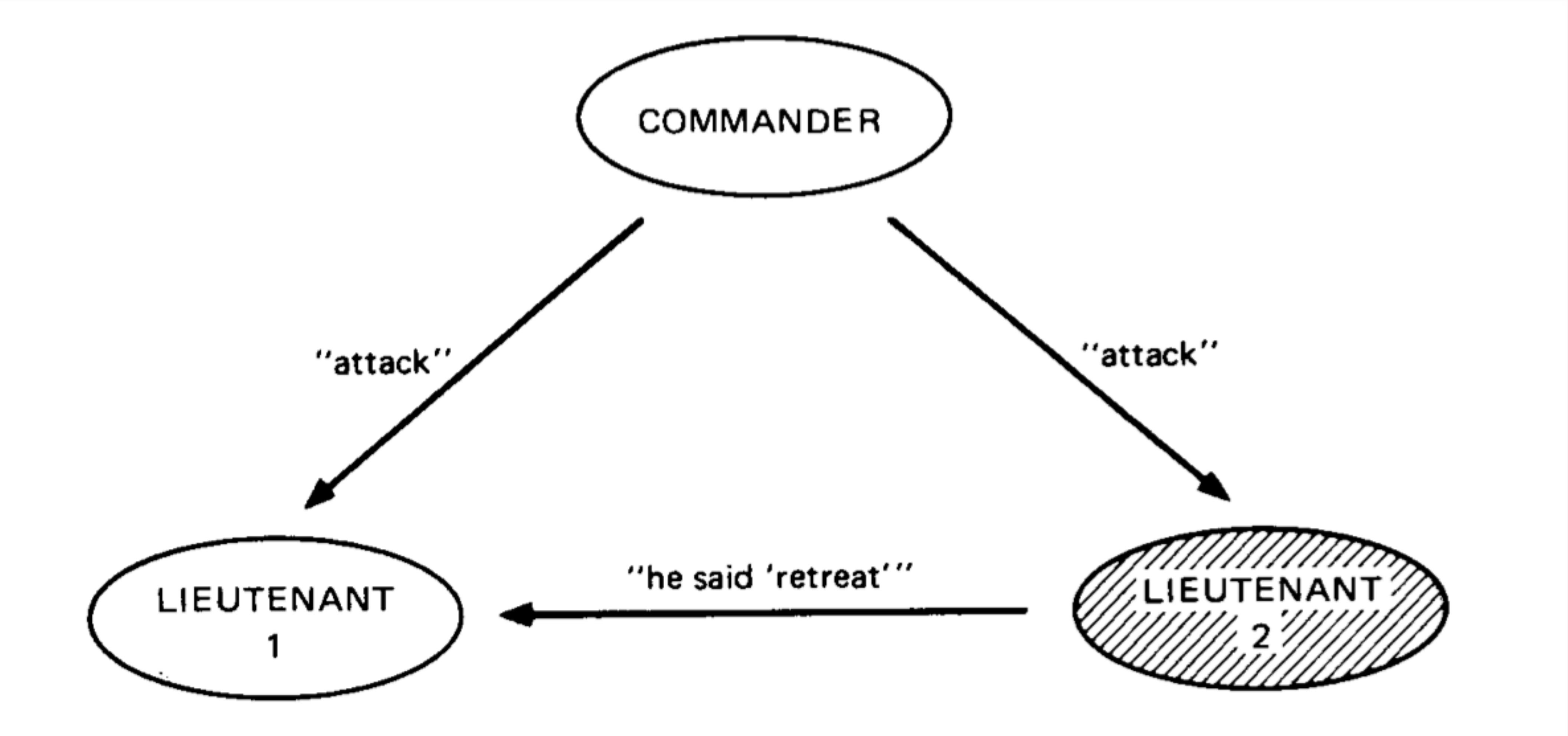
EARLY SOLUTIONS

- It is *Byzantine-fault-tolerant* as long as the number of disloyal generals is less than 1/3 of the generals.
- The problem can be reduced to solving a “Commander and Lieutenants” problem

EARLY SOLUTIONS



EARLY SOLUTIONS



EARLY SOLUTIONS

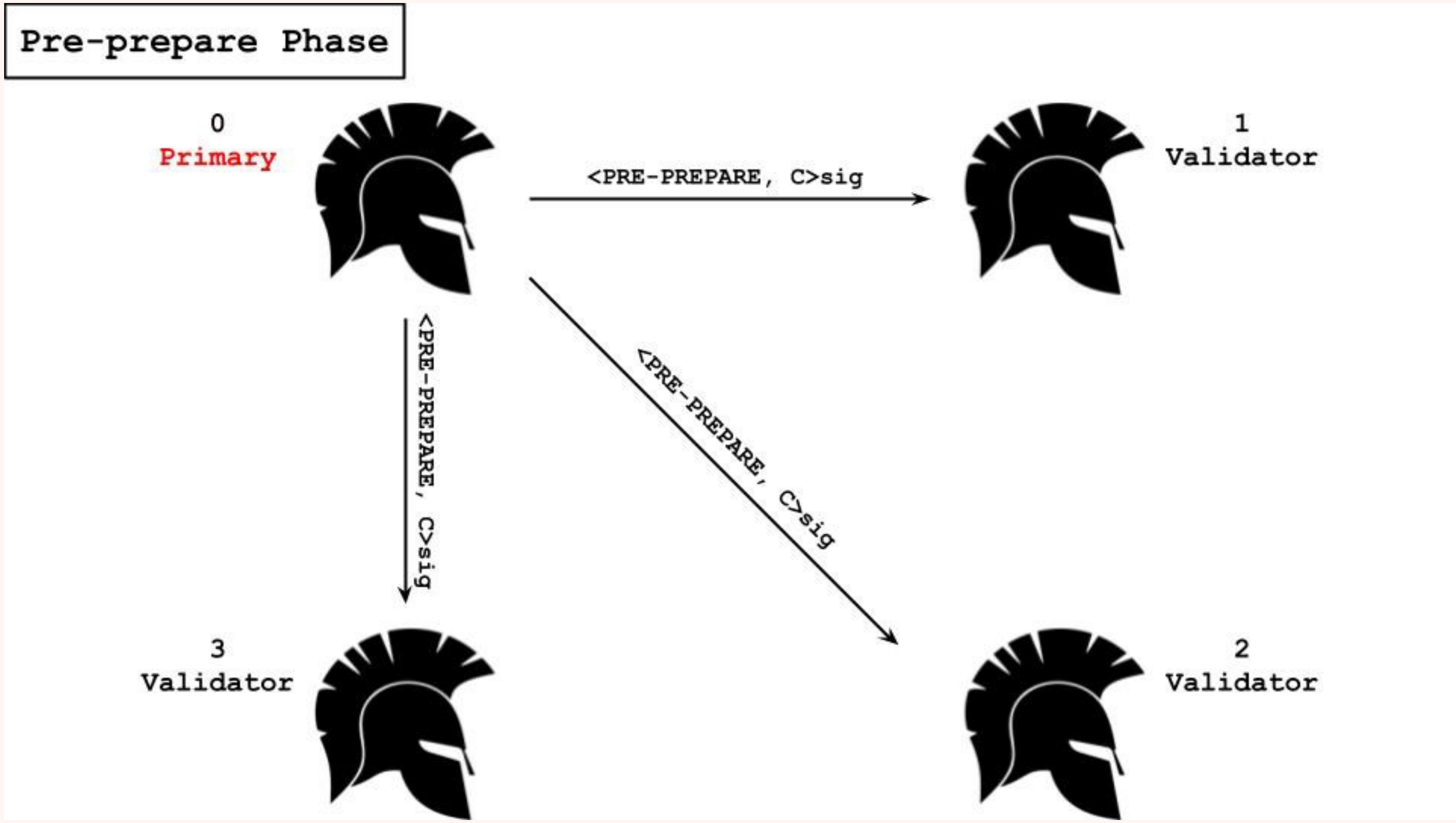
Problems?

- **It takes a lot of efforts to check the portion of the loyal/disloyal nodes.**

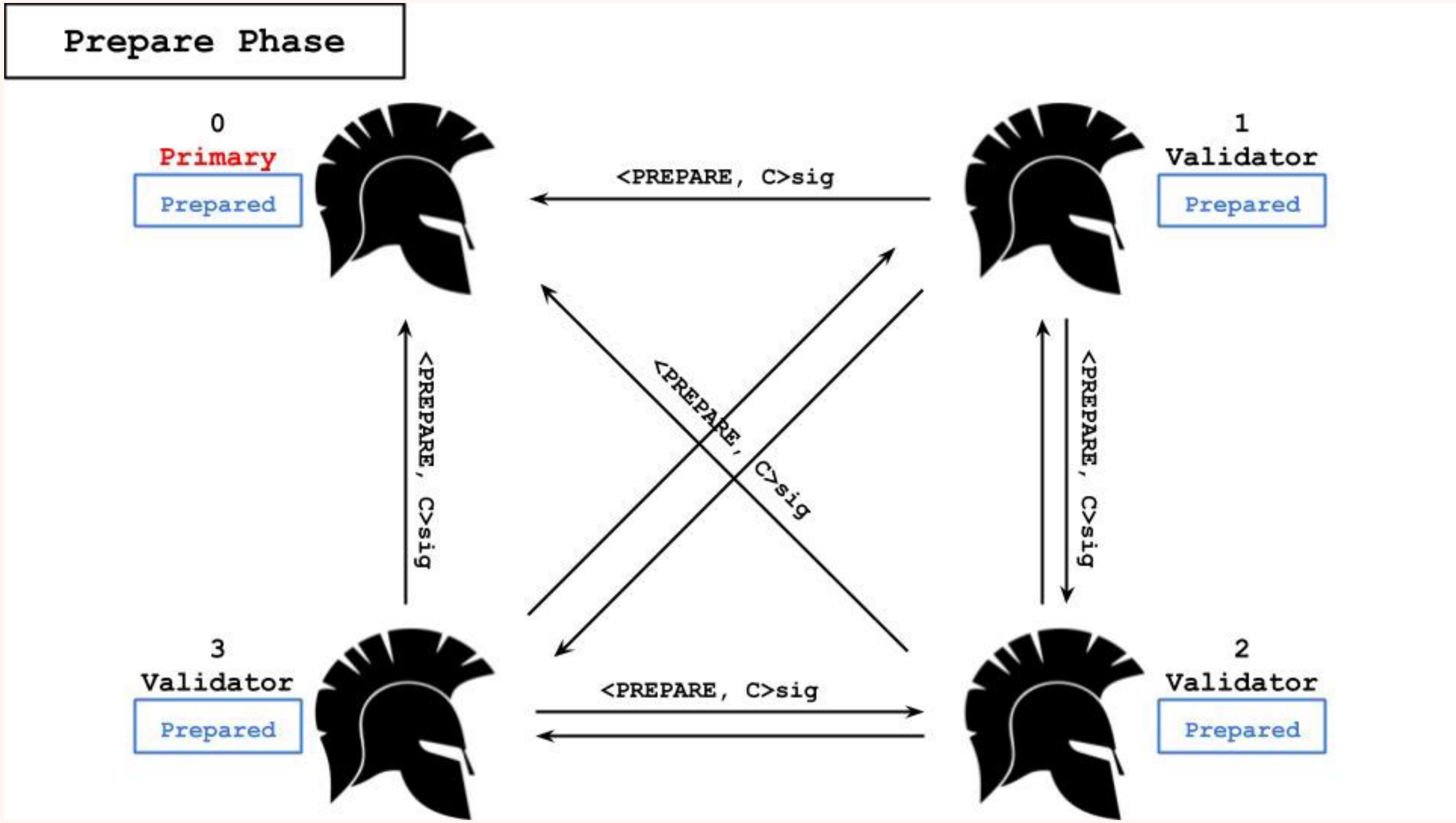
BYZANTINE FAULT TOLERANCE ALGORITHM

- **1999, Miguel Castro and Barbara Liskov —— “Practical Byzantine Fault Tolerance Algorithm (PBFT)”**
    - Secure and highly efficient
    - Pre-prepare →Prepare →Commit

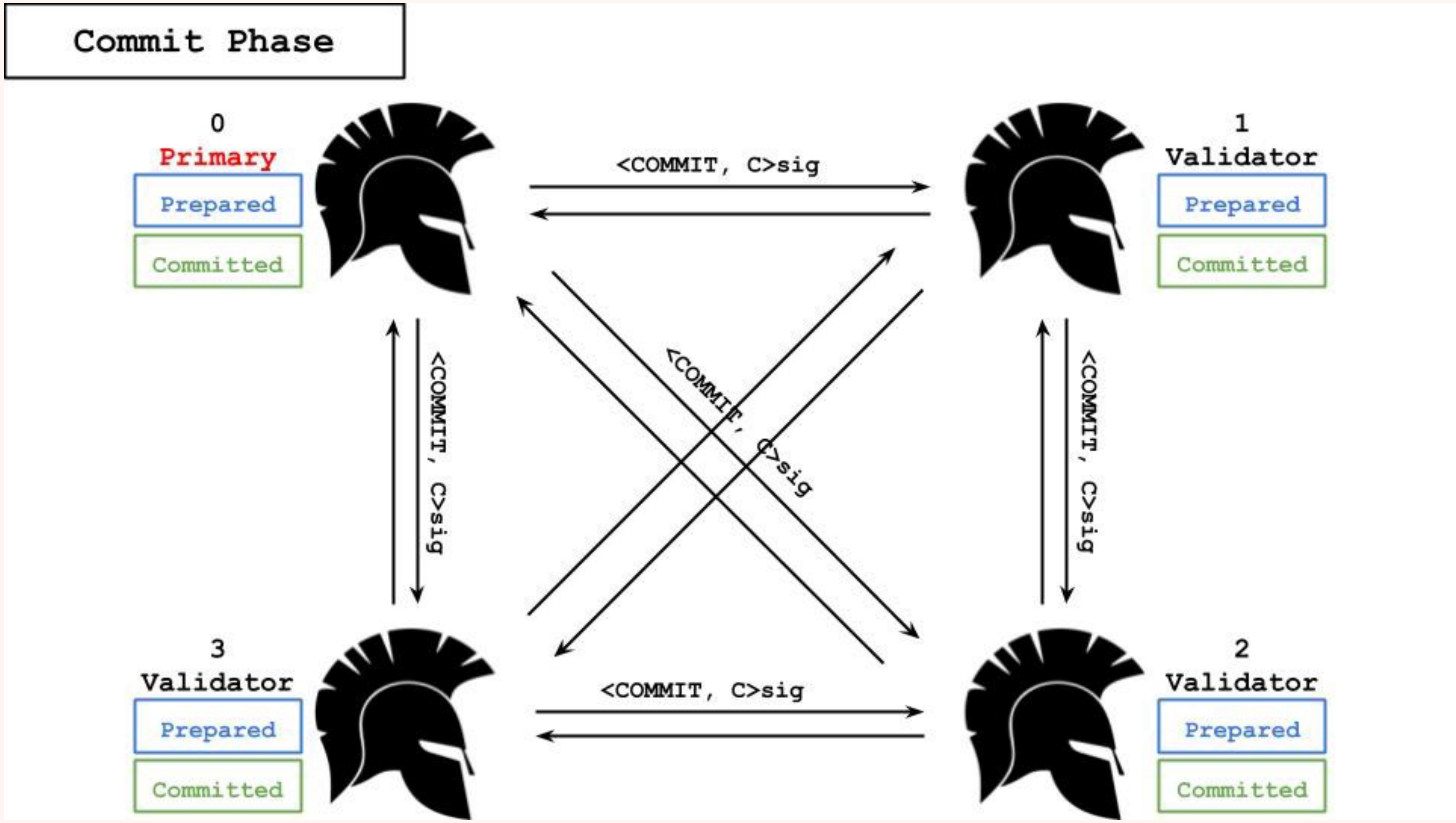
BYZANTINE FAULT TOLERANCE ALGORITHM



BYZANTINE FAULT TOLERANCE ALGORITHM



BYZANTINE FAULT TOLERANCE ALGORITHM



BYZANTINE FAULT TOLERANCE ALGORITHM

- **1999, Miguel Castro and Barbara Liskov —— "Practical Byzantine Fault Tolerance Algorithm"**
  - Secure and highly efficient
  - Pre-prepare →Prepare →Commit
  - View-change
- **And more……**

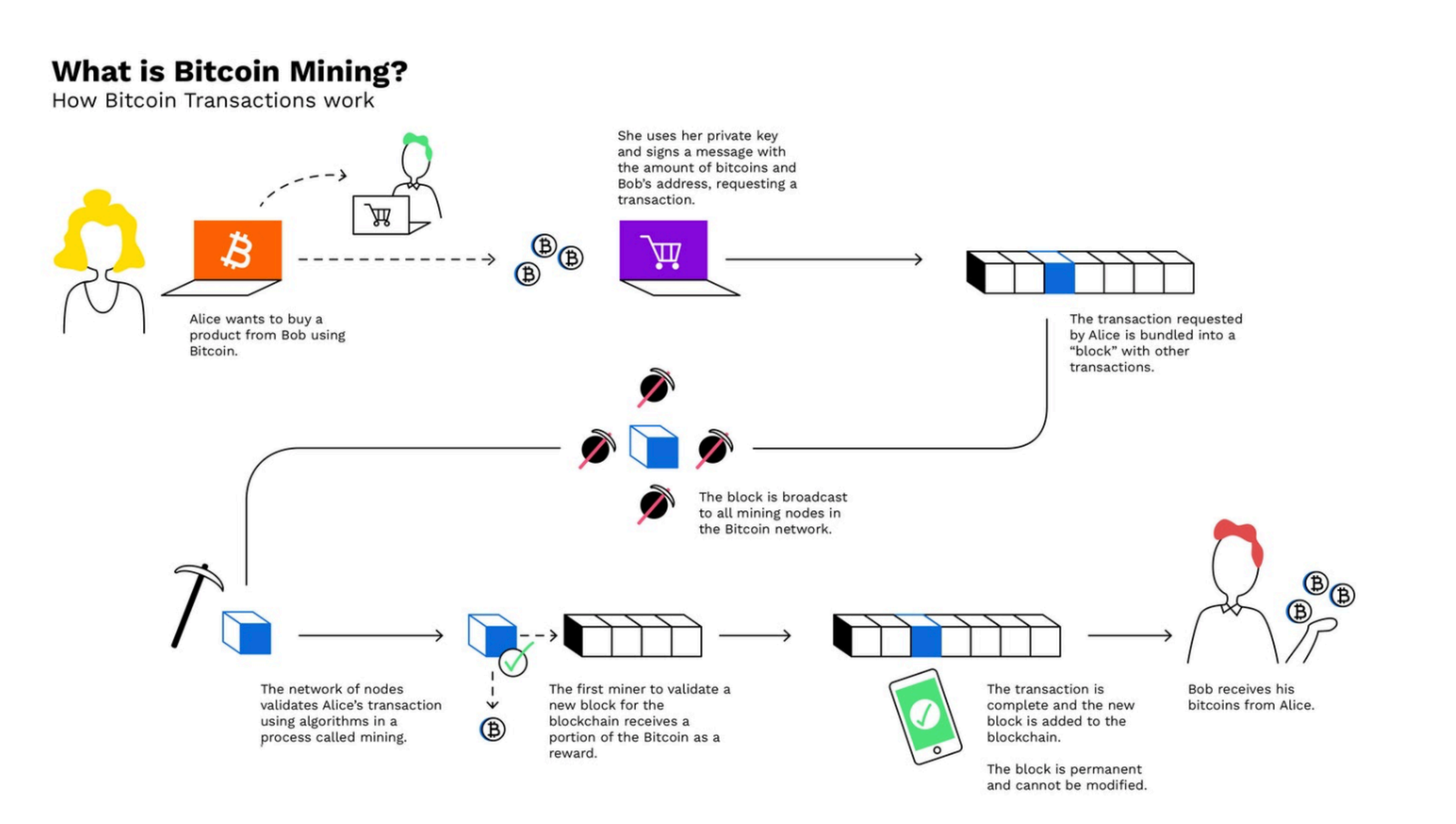
BITCOIN (₿)

- **In 2008, invented by Satomi Nakamoto (中本聰)**
- **A digital currency / cryptocurrency**
  - 2021/4/25 1 Bitcoin = 1,412,221.40 NTD
- **By using blockchain**
  - Owned and controlled by its user
  - Peer to peer, no centralized control

BITCOIN MINING

- Necessary to maintain the ledger of transactions upon which bitcoin is based
- The process of creating new bitcoin by solving a computational puzzle
- By solving computational math problems, bitcoin miners make the bitcoin payment network trustworthy and secure by verifying its transaction information

BITCOIN MINING



What is Bitcoin Mining?

How Bitcoin Transactions work

Alice wants to buy a product from Bob using Bitcoin.

She uses her private key and signs a message with the amount of bitcoins and Bob's address, requesting a transaction.

The transaction requested by Alice is bundled into a "block" with other transactions.

The block is broadcast to all mining nodes in the Bitcoin network.

The network of nodes validates Alice's transaction using algorithms in a process called mining.

The first miner to validate a new block for the blockchain receives a portion of the Bitcoin as a reward.

The transaction is complete and the new block is added to the blockchain.

The block is permanent and cannot be modified.

Bob receives his bitcoins from Alice.

WHAT’S NEXT?

- Quantum computer’s crisis?
- Other cryptocurrency…

REFERENCE

- IBM - What is blockchain Technology (https://www.ibm.com/topics/what-is-blockchain)
- LAMPORT, LESLIE, ROBERT SHOSTAK, and MARSHALL PEASE. "The Byzantine Generals Problem." *ACM Transactions on Programming Languages and Systems* 4.3 (1982): 382-401.
- Investopedia - How Does Bitcoin Mining Work (https://www.investopedia.com/tech/how-does-bitcoin-mining-work/)
- Bitpanda Academy (https://www.bitpanda.com/academy/en)
- Taipei Ethereum Meetup(https://medium.com/taipei-ethereum-meetup/intro-to-pbft-31187f255e68)