SWINBURNE UNIVERSITY OF TECHNOLOGY

Theory of Blockchain

Session 5:

Fundamentals of Blockchain

Module 1 – Byzantine Generals Problem

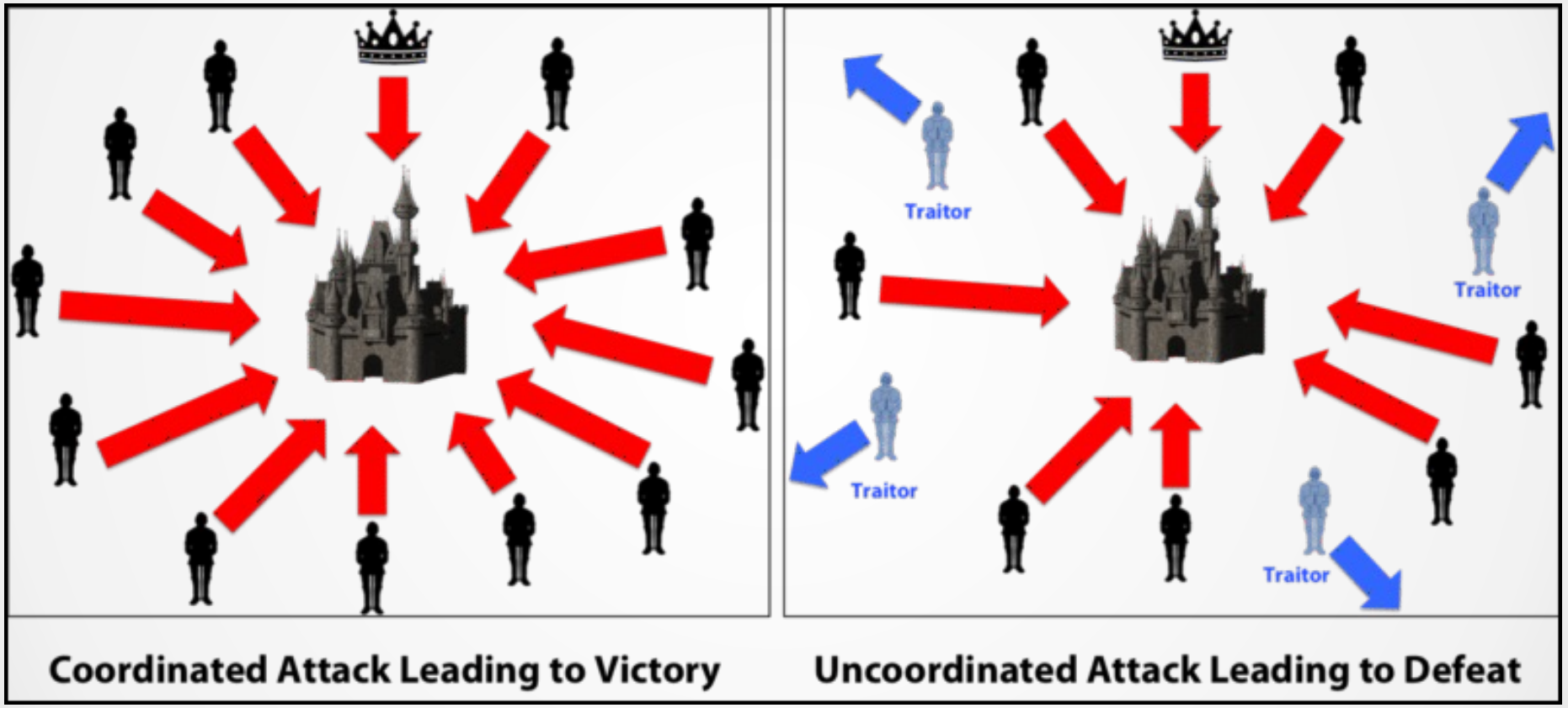
What did Bitcoin Solve?

Bitcoin practically gave a solution to the distributed consensus problem, which was around for many years.

- It also had a brilliant idea on how to order the agreed events.

The scientific problem underneath is called **“The Byzantine Generals’ Problem”.**

The Byzantine Generals' Problem



(Medium)

Highly suggested video: https://www.youtube.com/watch?v=dfsRQyYXOsQ

The Problem

- You can’t fully trust your generals, as there can be traitors among them.
- You can’t fully rely on messengers either, as they can be captured.

Questions:

- Will you ever reach consensus?
- How many traitors can you “tolerate” in your network at most?

2 Generals Problem

A

B

A wants to attack

If you respond, I will attack at dawn

A will attack
B wants to attack

If you respond, I will attack too

A will attack
B will attack

Okay, we will attack

A will attack
B will attack

Okay, we will attack

.
.
.

Byzantine Generals Problem

Paper: "The Byzantine Generals Problem", L. Lamport, R. Shostack, M. Peace, ACM TOPLAS, 1982.

Answers:

- How many byzantine node failures can a distributed system tolerate?
- How can you build such a system?

n=3

There’s no solution to the Byzantine 3 Generals 1 Traitor Problem

Commanding general

Retreat

?

Attack

general

Attack

general

Commanding general

Attack

?

general

Attack
Retreat

general

How many traitors are tolerated?

Reference paper's Theorem:

There's no solution for **3m+1** generals with **>m** traitors.

- Proof is done by contradiction i.e. using a hypothetical solution and reduction of it to solve the 3 generals 1 traitor problem.

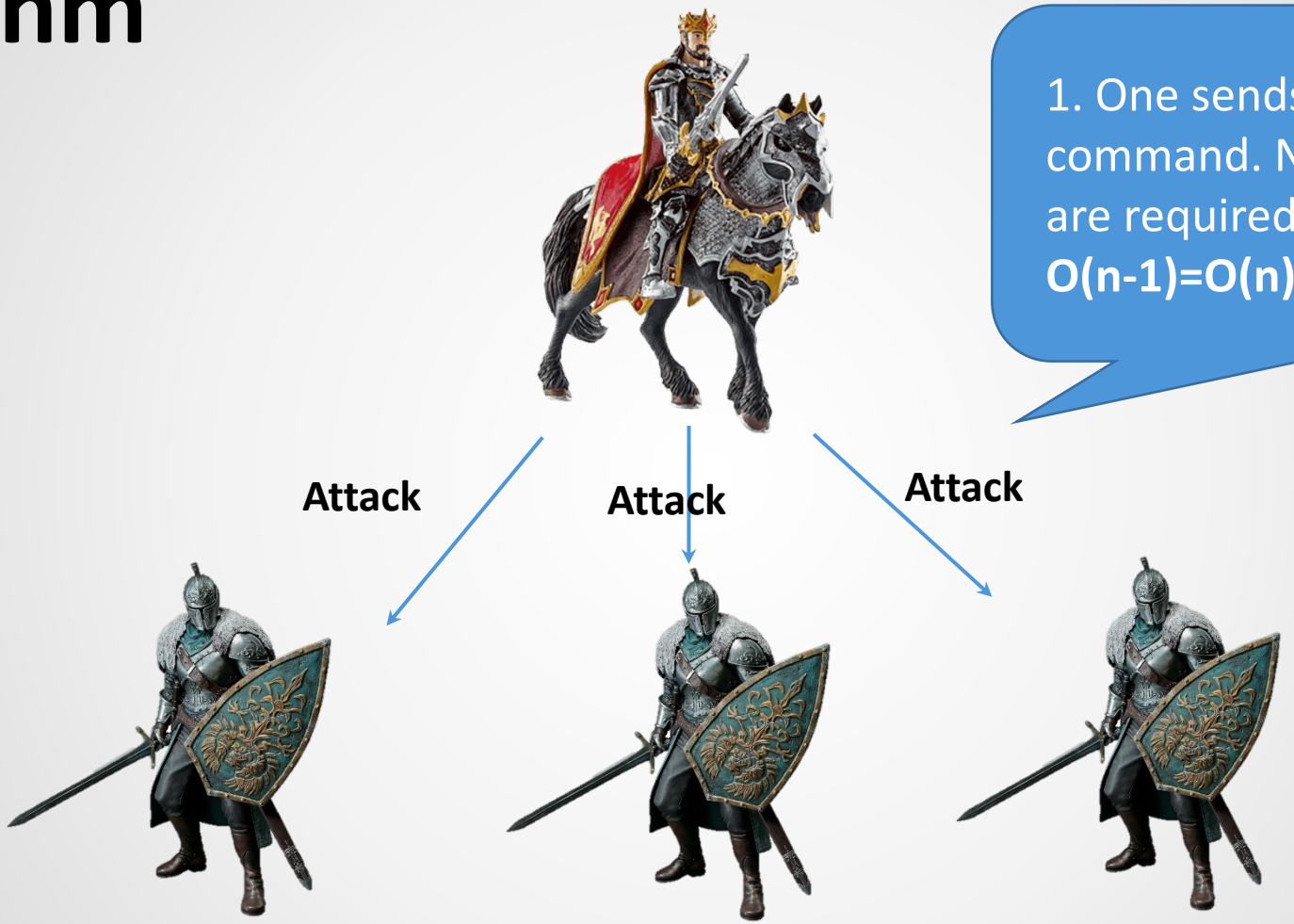
Oral (full gossip) Message Algorithm (for BGP)

- Assumptions:
  - Less than 1/3 of the generals are traitors.
  - Oral Messages
  - No Cryptography

Inductive Solution for Oral Message Algorithm

m=0

n=4

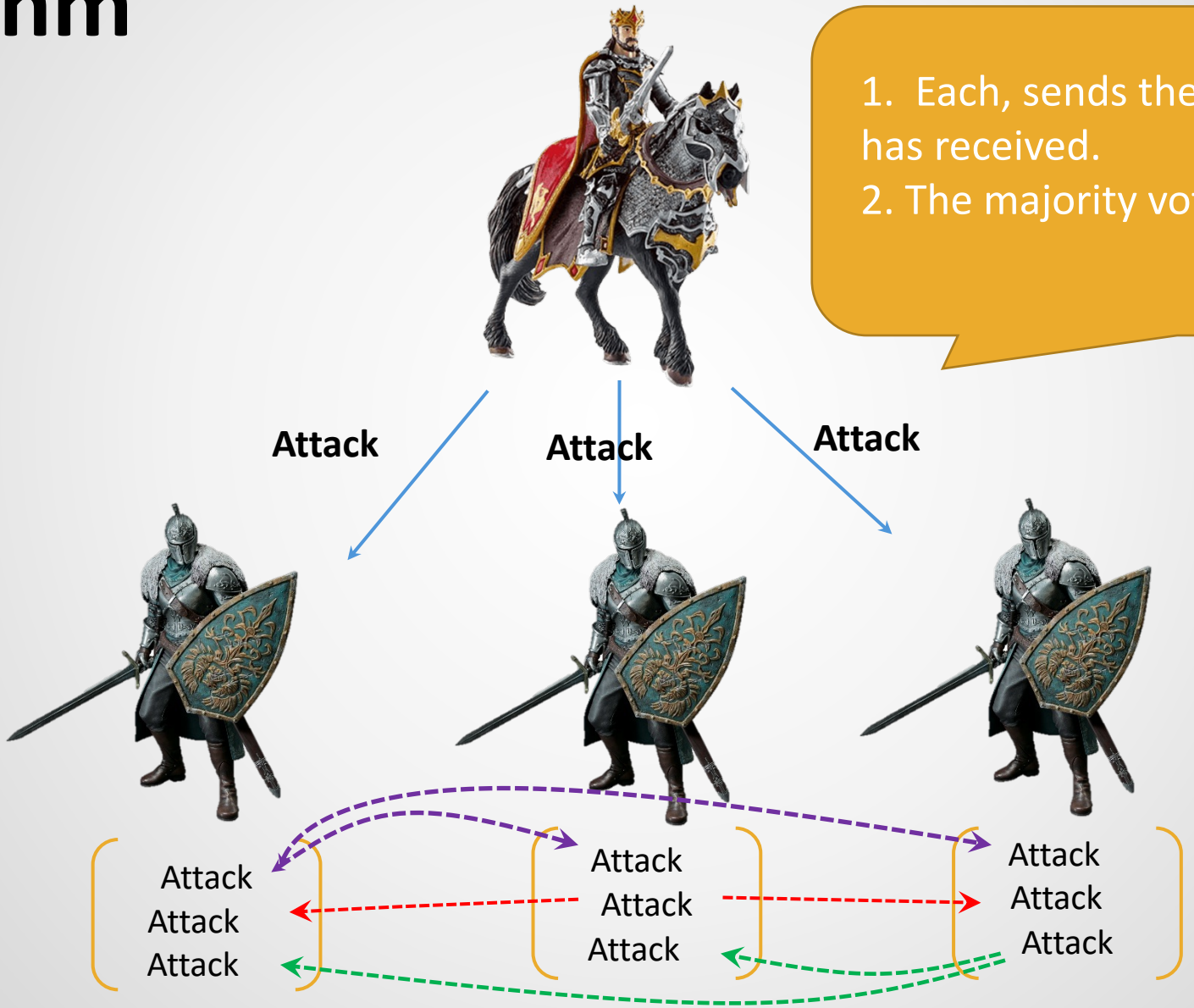


1. One sends the others the command. No more messages are required.
O(n-1)=O(n)

Inductive Solution for Oral Message Algorithm

m=1

n=4



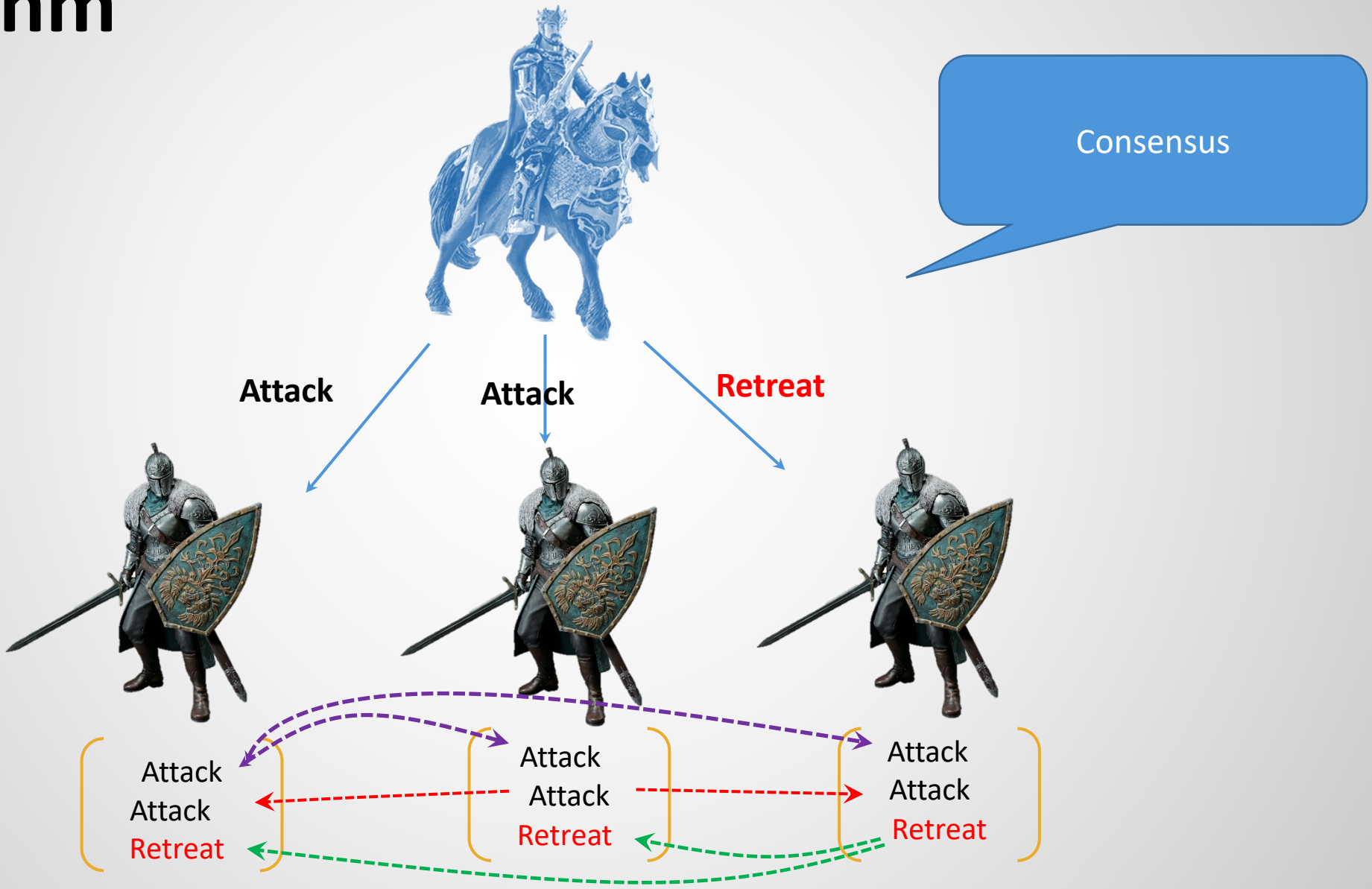
1. Each, sends the n-1 others the copy it has received.
2. The majority vote → consensus.

O(n^2)

Inductive Solution for Oral Message Algorithm

m=1

n=4



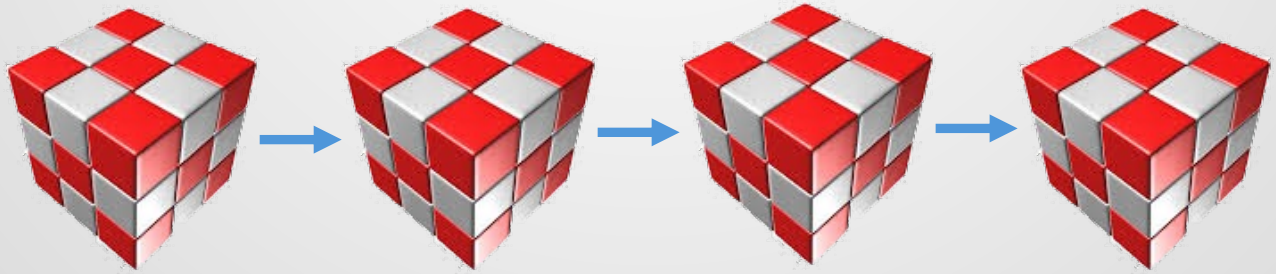
Running Complexity of Oral Message Algorithm

m traitors	Message Overhead
0	$O(n)$
1	$O(n^2)$
2	$O(n^3)$
3	$O(n^4)$
…	…

We didn't have crypto here. Cryptography can help a bit.

So, What is Blockchain?

Blockchain is a secure transaction ledger database (initially made to facilitate currency exchanges) shared by all the members participating in a distributed network of computers. (LSTA)



What Comes Next …

- We learned about the fundamental problem of consensus in a distributed environment.
- We presented the gossiping solution to Byzantine Generals' problem and showed the resistance thresholds.
- In the next video, we explain the basics of distributed ledger and transaction ordering.

See you in the next video …