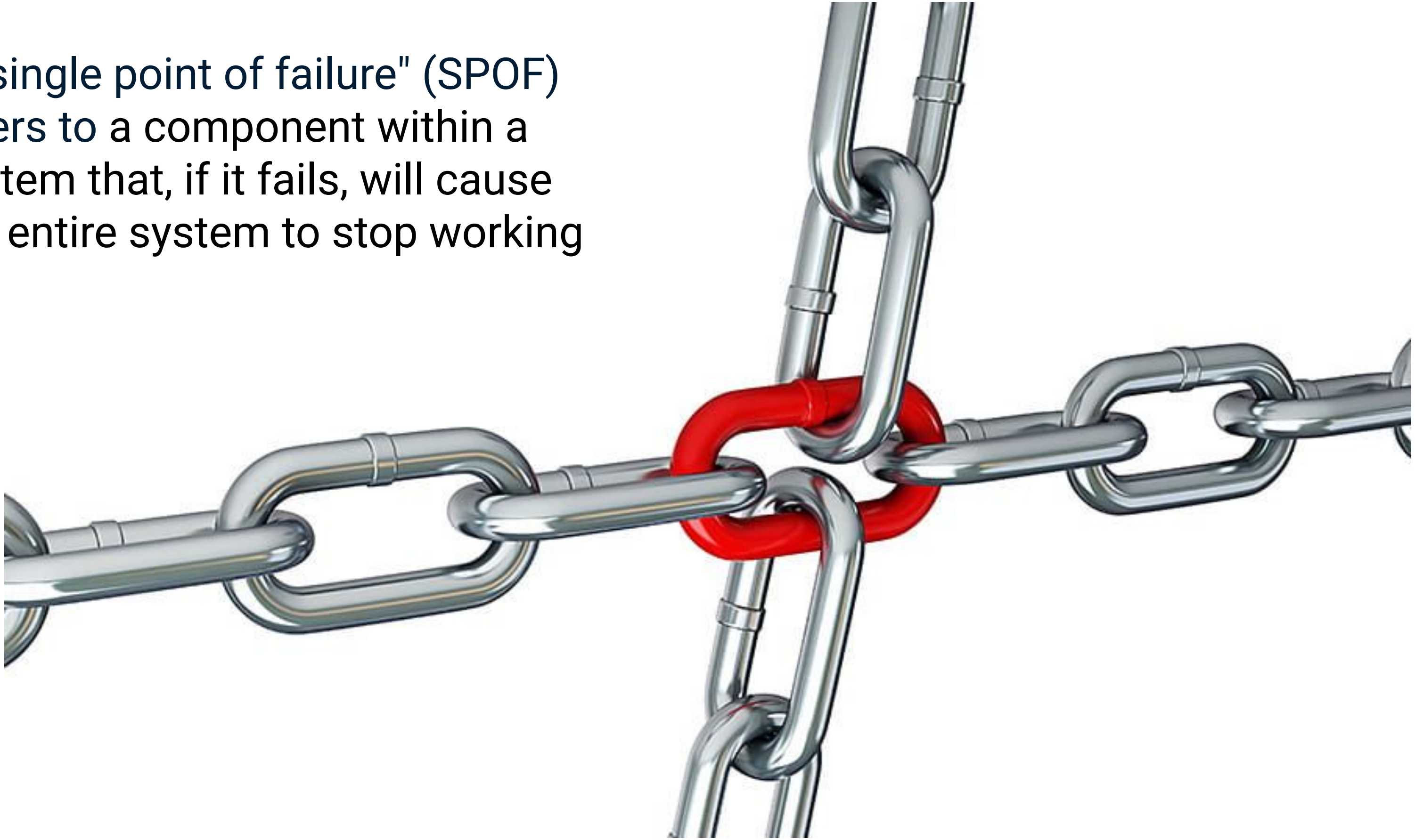
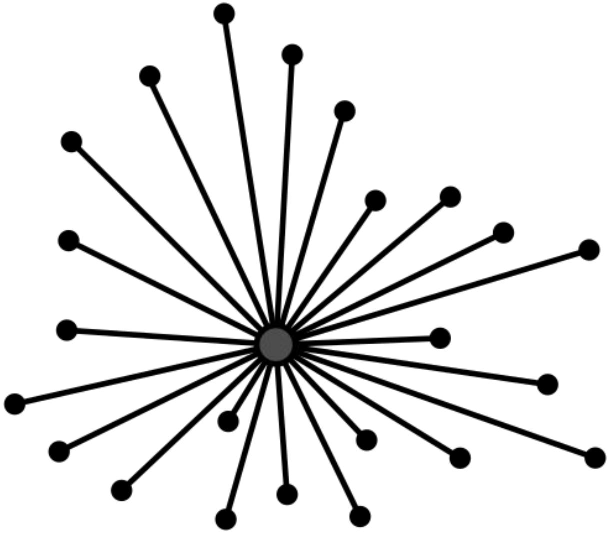
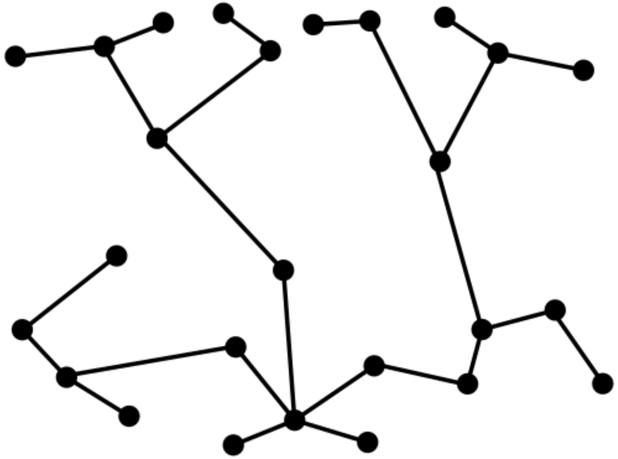
CSC 116 **Single Point of Failure & BFT**

A "single point of failure" (SPOF) refers to a component within a system that, if it fails, will cause the entire system to stop working





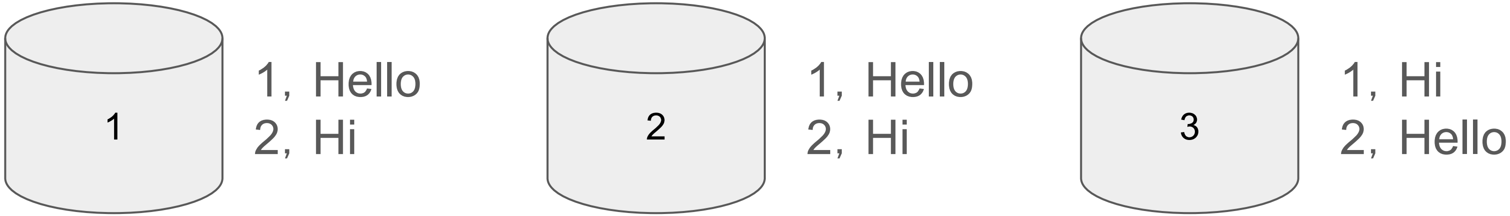
CENTRALIZED



DECENTRALIZED

What we need to learn today：

How to make sure that all the datasets in different servers are the same datasets?

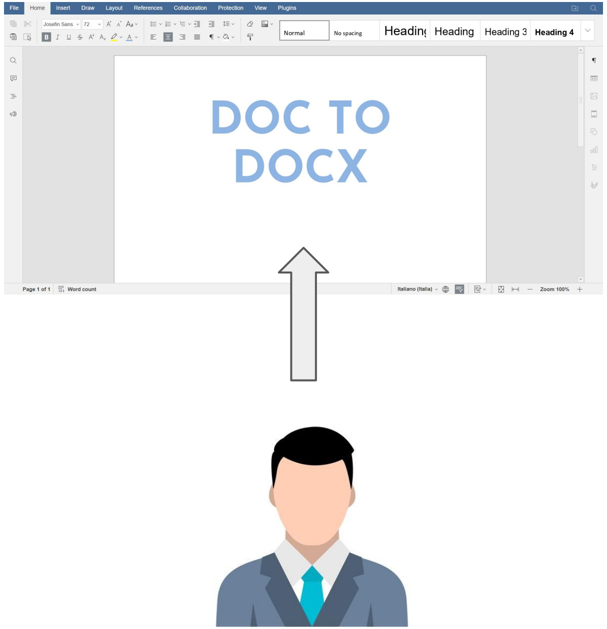


1, Hello
2, Hi

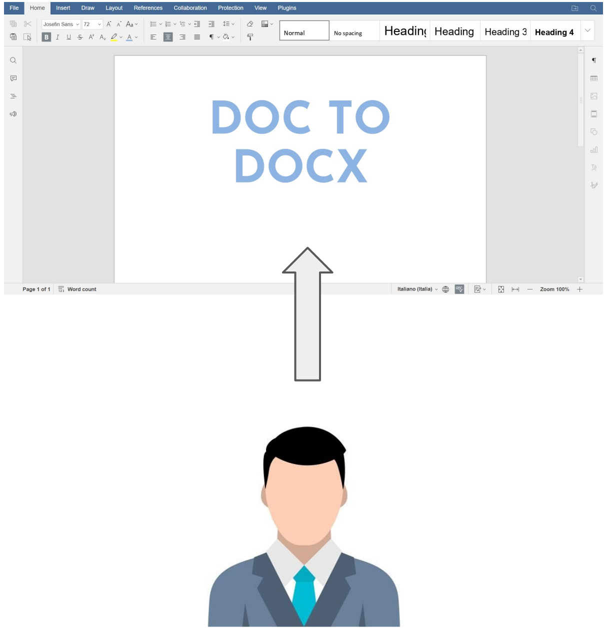
1, Hello
2, Hi

1, Hi
2, Hello

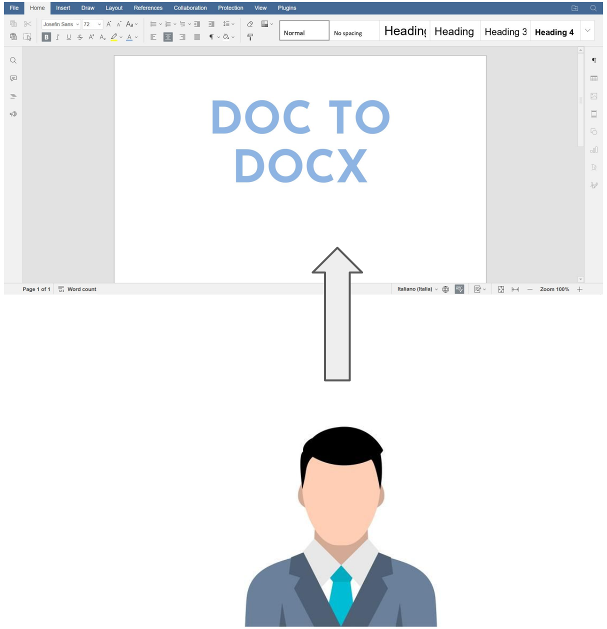
Google Docs



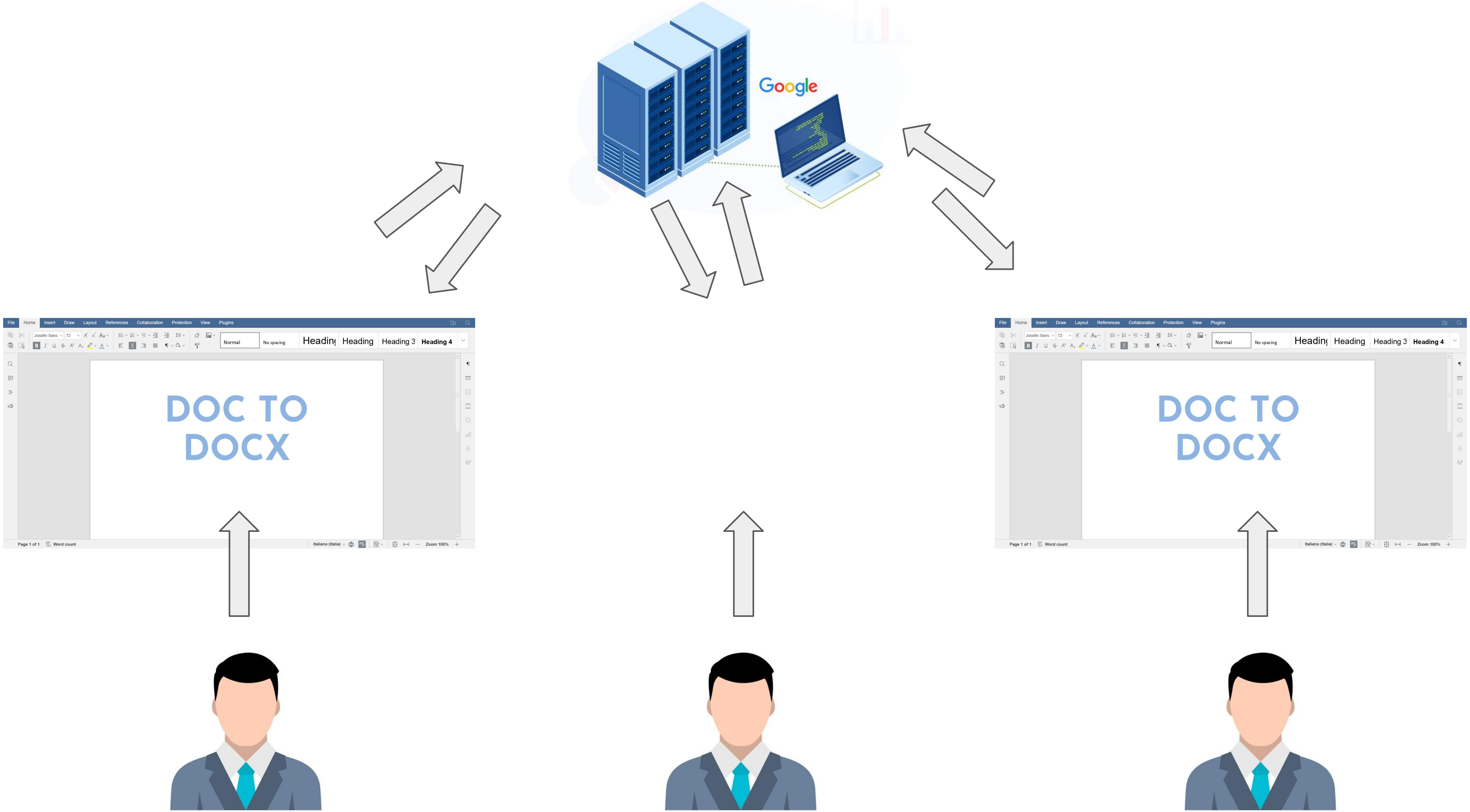
DOC TO DOCX



DOC TO DOCX



DOC TO DOCX


Google
File
Home
Insert
Draw
Layout
References
Collaboration
Protection
View
Plugins
Josefin Sans
72
Normal
No spacing
Heading
Heading
Heading 3
Heading 4
DOC TO DOCX
Page 1 of 1
Word count
Italiano (Italia)
Zoom 100%
File
Home
Insert
Draw
Layout
References
Collaboration
Protection
View
Plugins
Josefin Sans
72
Normal
No spacing
Heading
Heading
Heading 3
Heading 4
DOC TO DOCX
Page 1 of 1
Word count
Italiano (Italia)
Zoom 100%

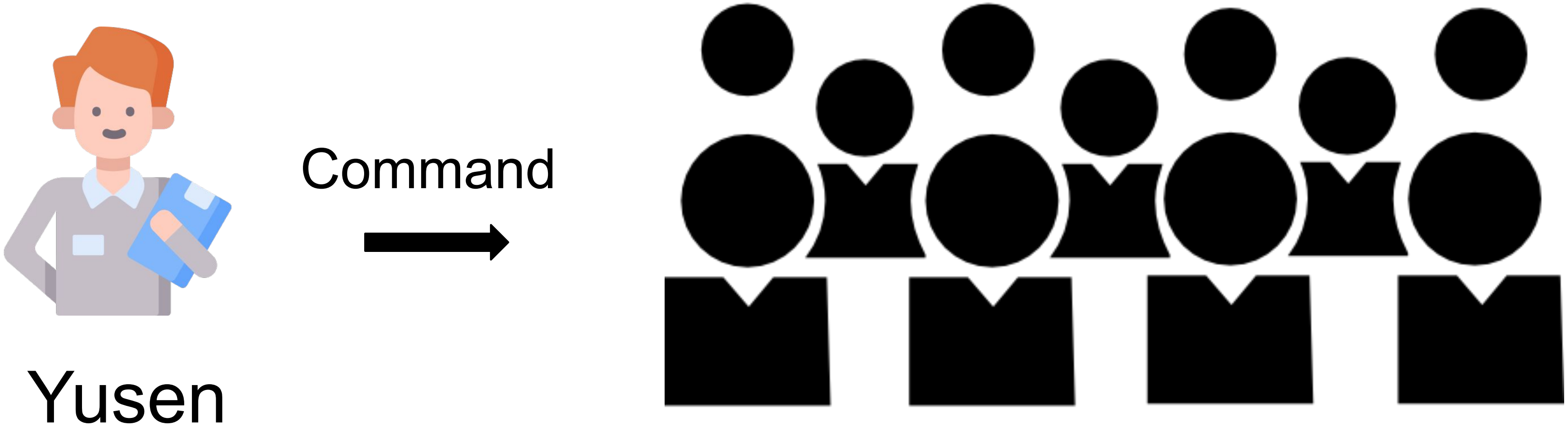
BFT

(Byzantine Fault Tolerance)

It’s an algorithm!

Fake news!

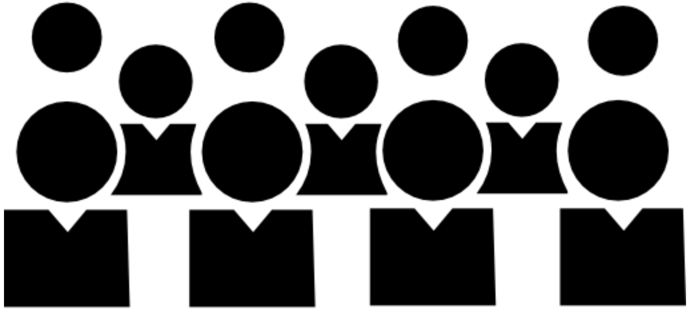
You don’t need to complete the assignment 2,
I will give you 8% for free.



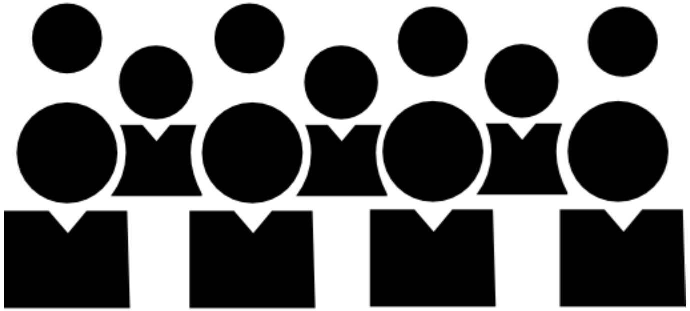
Command

Yusen

1. Yusen is a global unique hash code!



2. You are all real AI models. Your brains tell you: 1). Yusen is a real person and he is the instructor of this course. 2) He is in the class, we are face to face, 3). I clearly hear what he said in the classroom.



All of you in this classroom will
trust that this is a real command.
But the students not here may
not trust. It should be a joke!!

Let’s make some conclusions:

What you find in this game?

Consensus

1 Your eyes record all the students, they are all evidences

2 You heard the leader’s command, and the leader is trusted (I am a real instructor)

3 Your brain tells you it is true

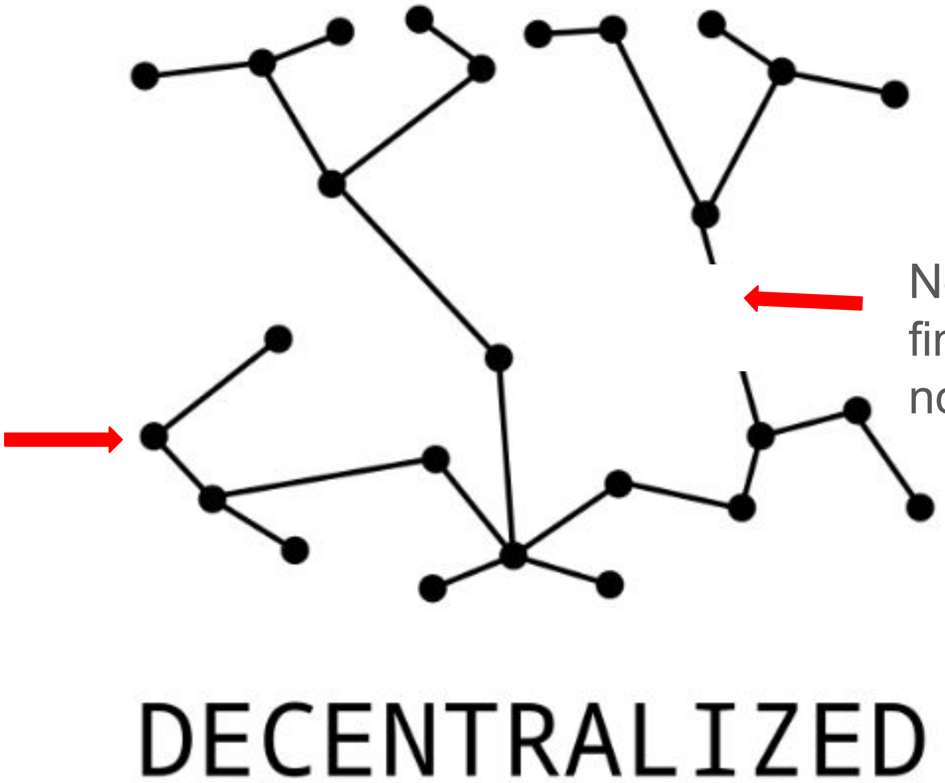
Other Students May not Trust you

1 You are not a leader, it sounds not real

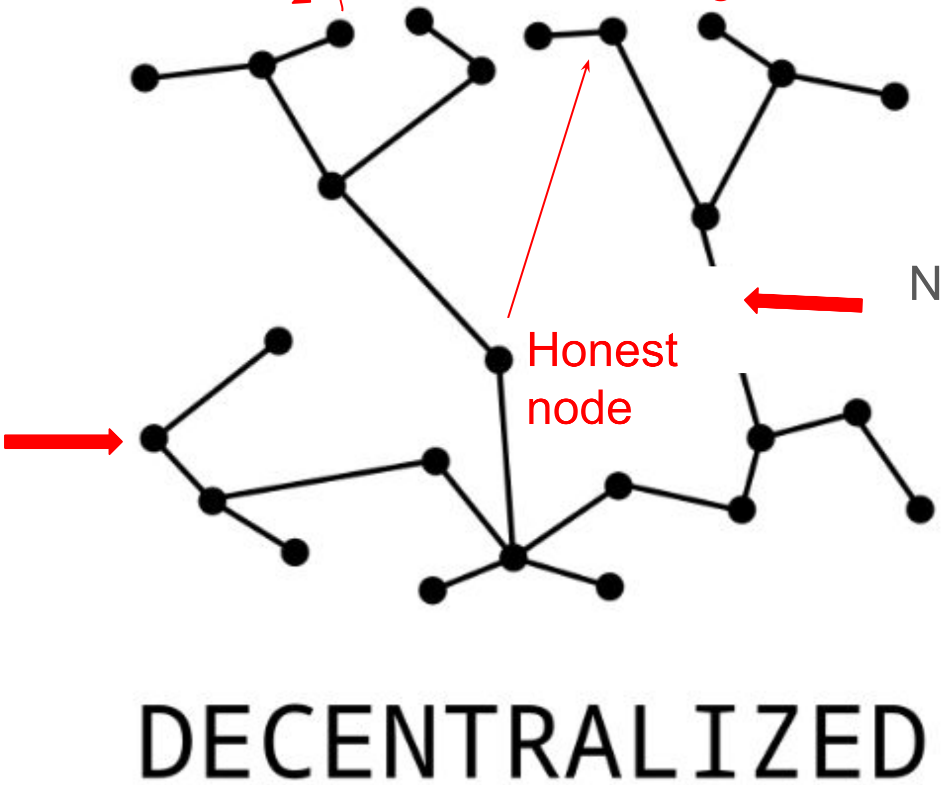
2 You may be joking

3 They are not in the classroom, they did not hear it and experience it.

BFT feature：Must send the message by a leader



Network broken! But it is fine. Because majority nodes are honest nodes

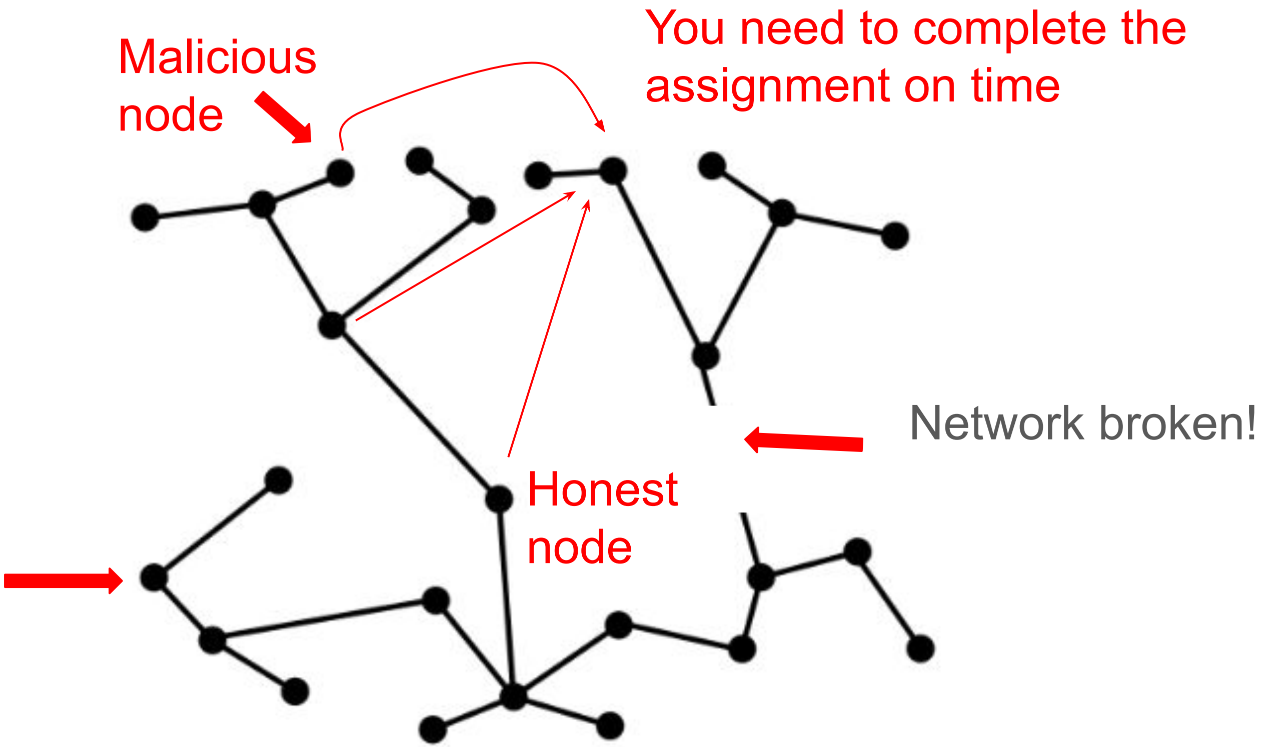


Malicious node

You need to complete the assignment on time

Honest node

Network broken!



Malicious node

You need to complete the assignment on time

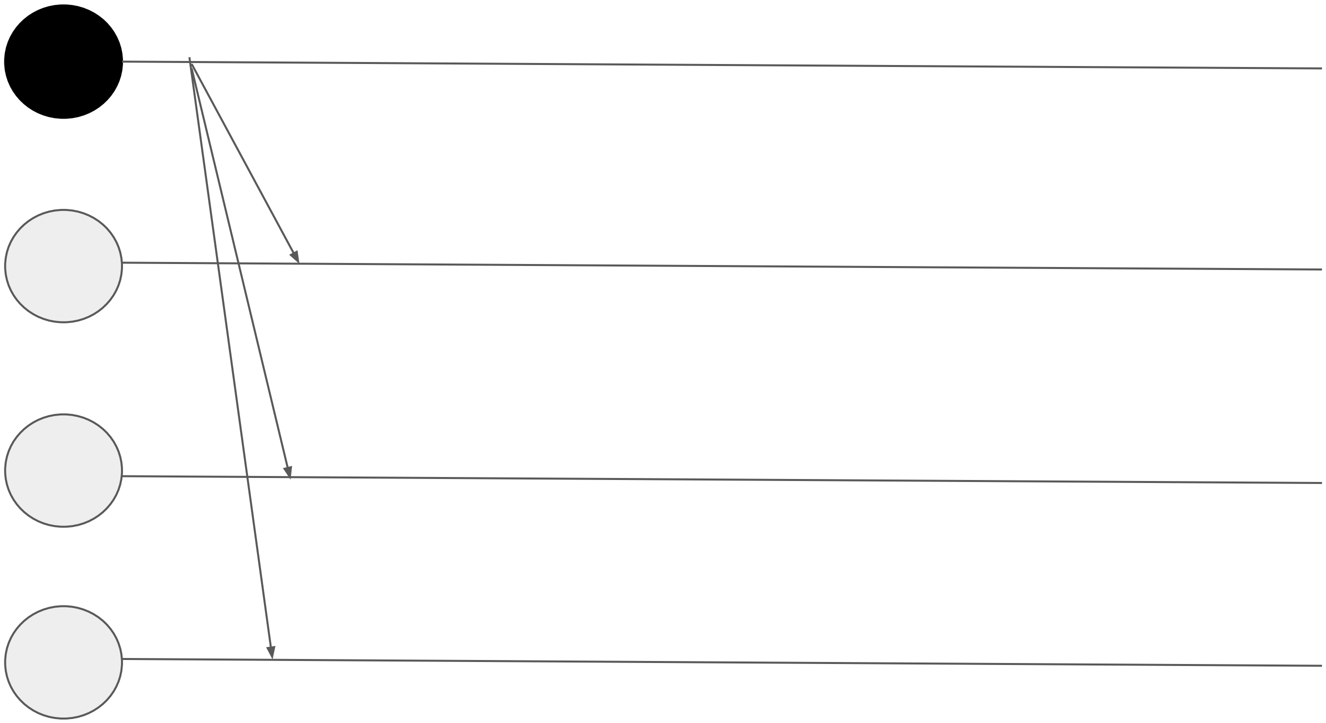
Network broken!

Honest node

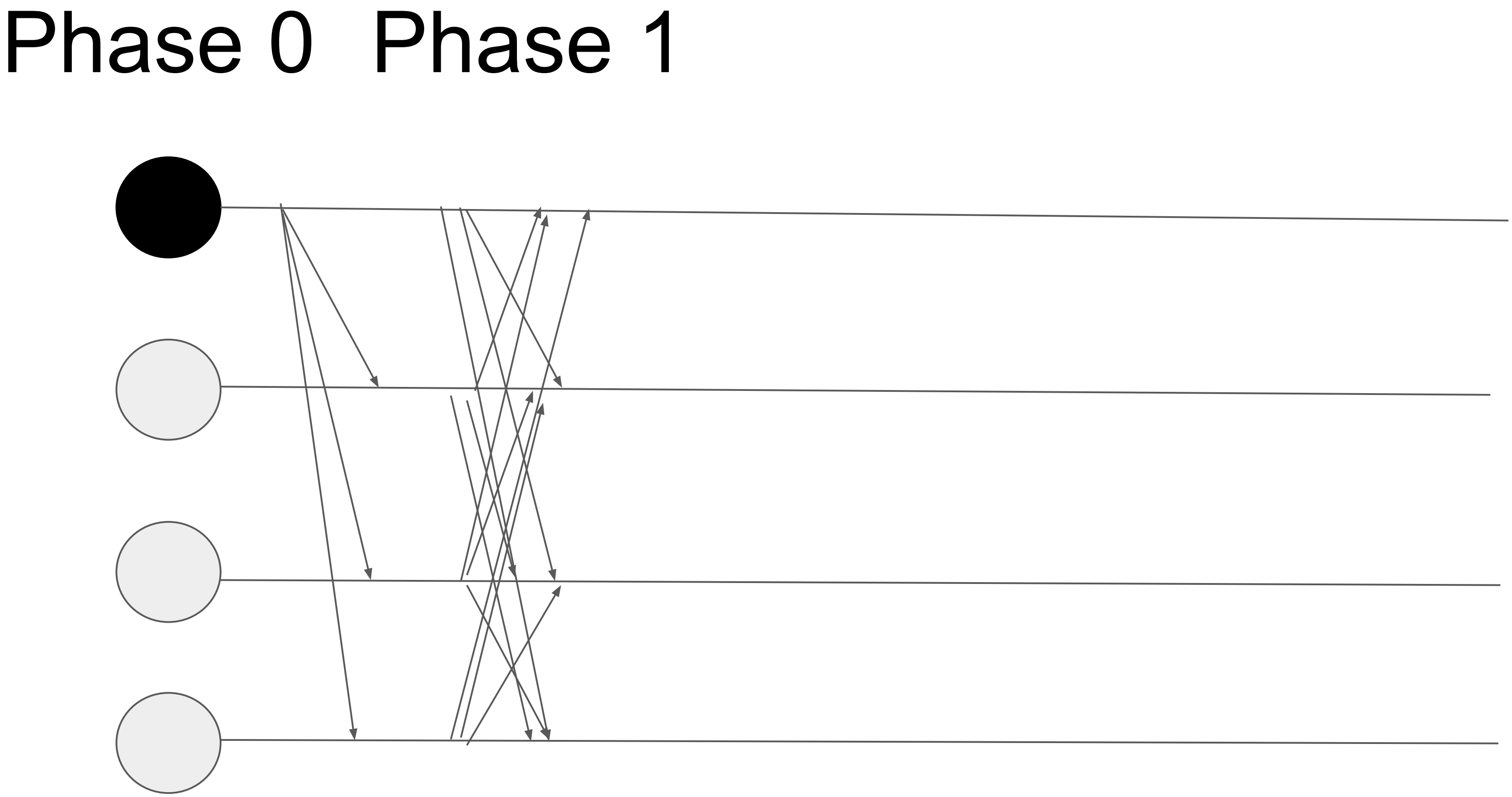
DECENTRALIZED

Phase 0: Leader broadcast messages to all the students (nodes)

Phase 0



Phase 1: All the nodes start to broadcast messages


Phase 0
Phase 1

Why need to broadcast messages？

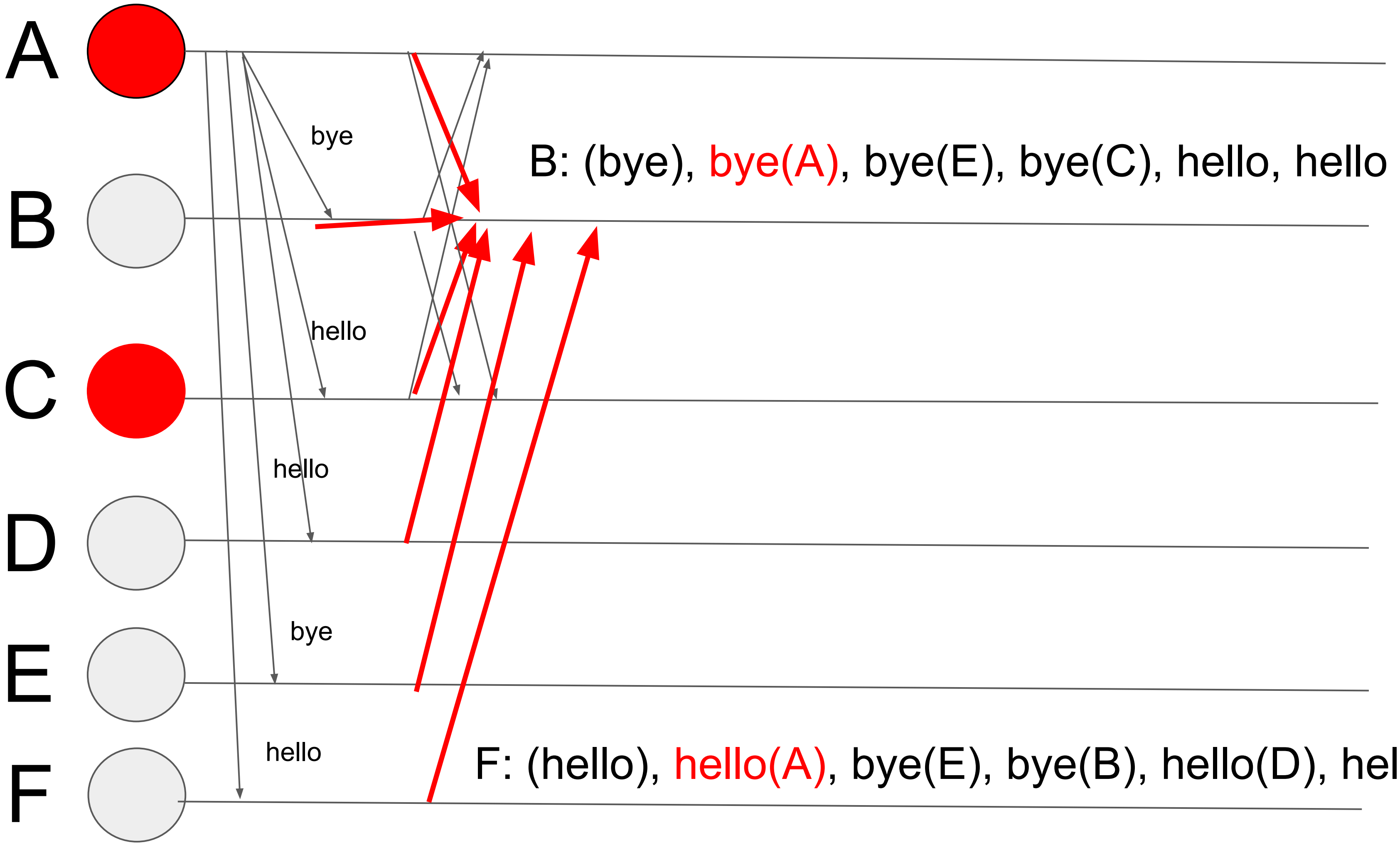
n: total nodes

f: total number of malicious nodes

n - f > f : the number of correct students needs to large than the number of malicious students.

$$\mathbf{n > 2f}$$

$$\color{red}{\mathbf{n >= 2f + 1}}$$

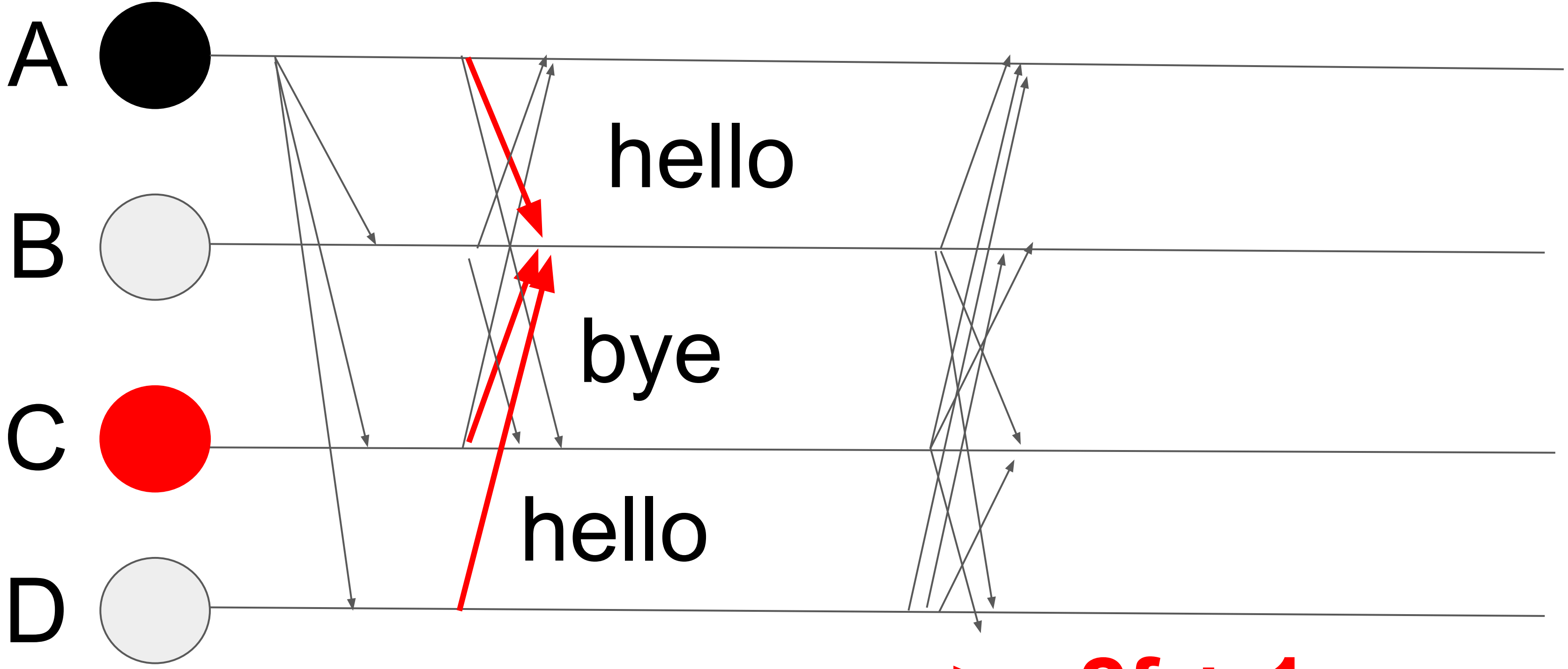


B: (bye), bye(A), bye(E), bye(C), hello, hello

F: (hello), hello(A), bye(E), bye(B), hello(D), hello(C)

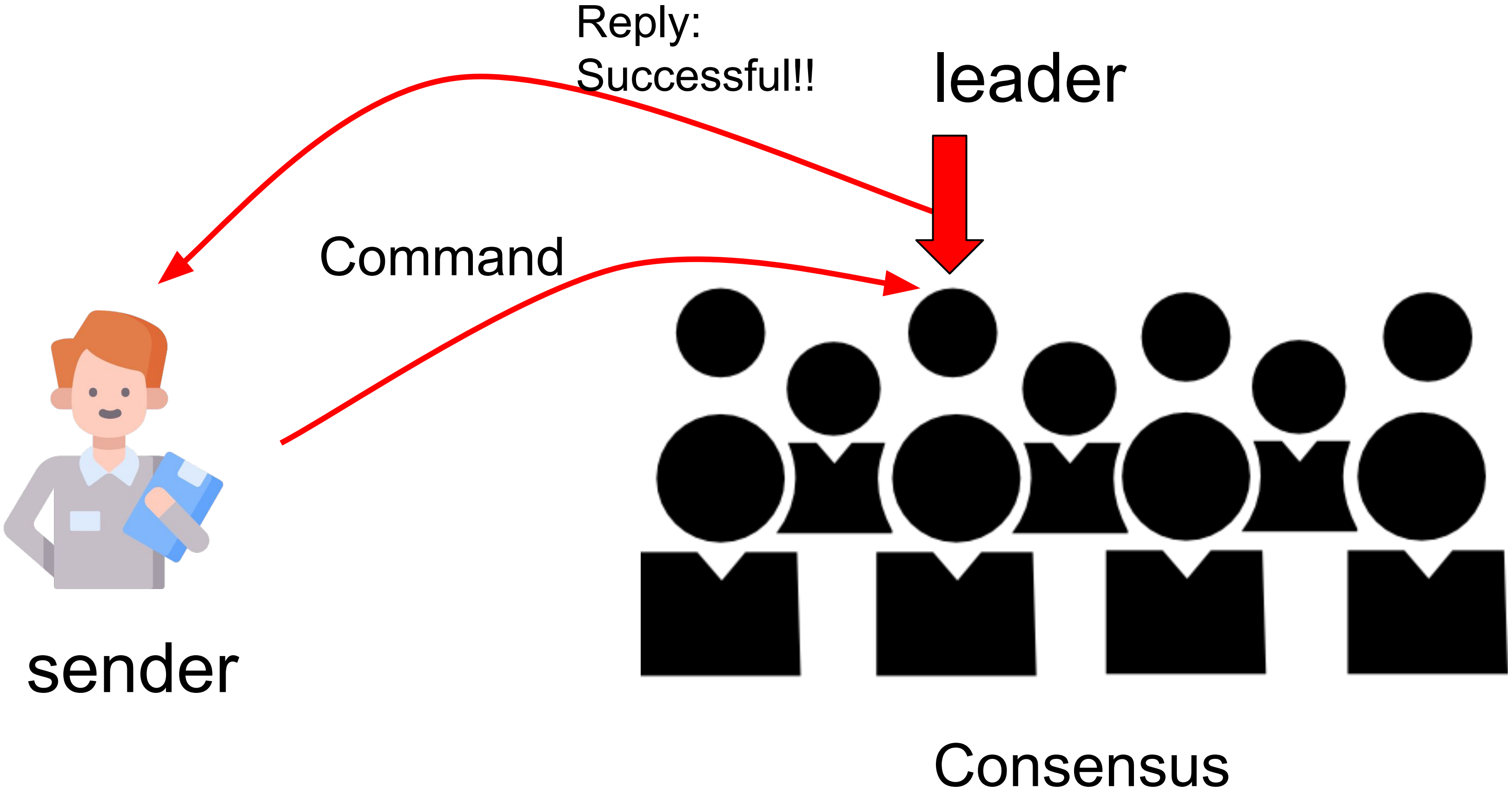
Phase 2: Confirm the Message to everyone and leader

Phase 2



n >= 2f + 1

Totality: Total order



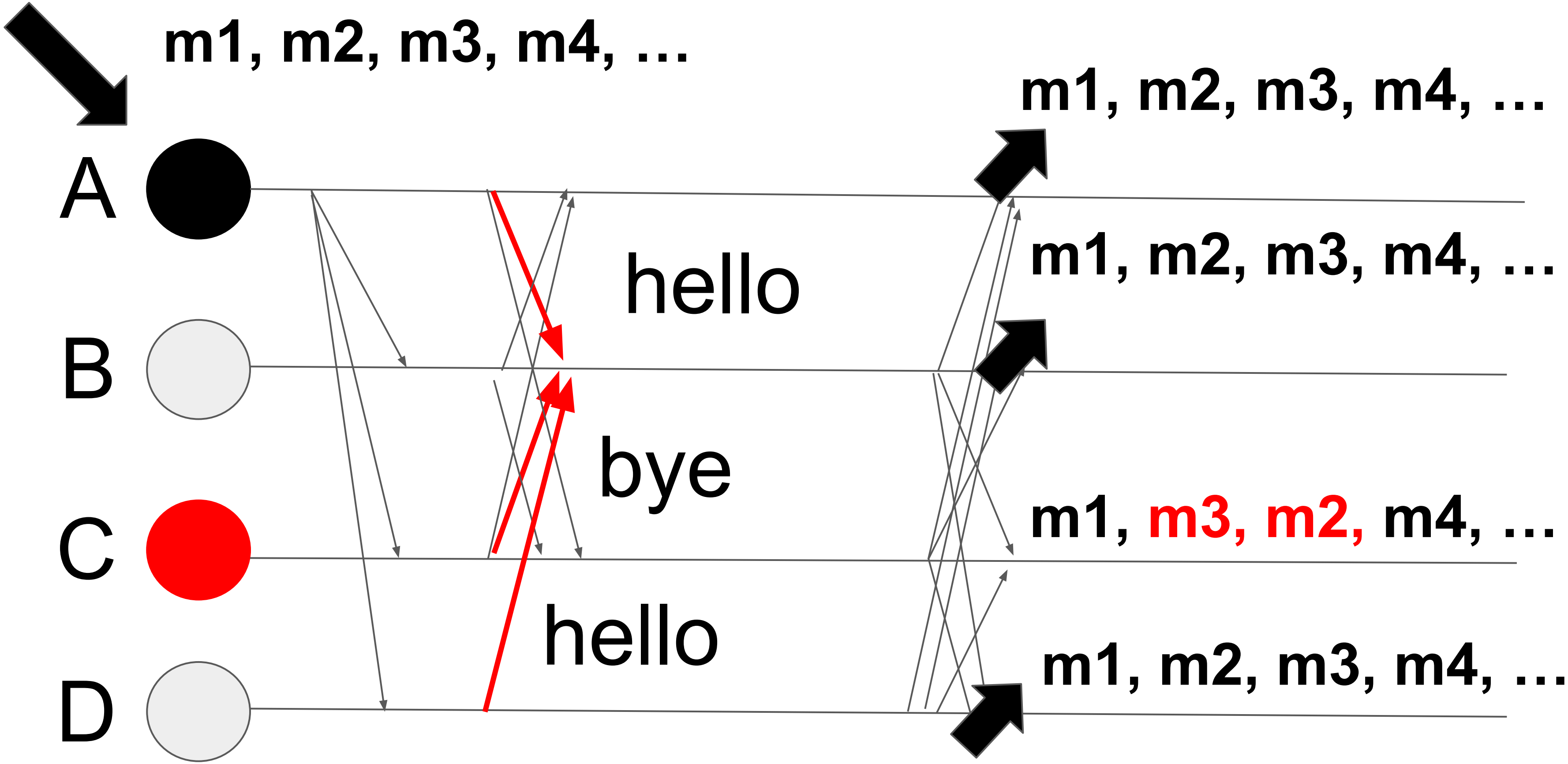
Reply:
Successful!!

leader

Command

sender

Consensus



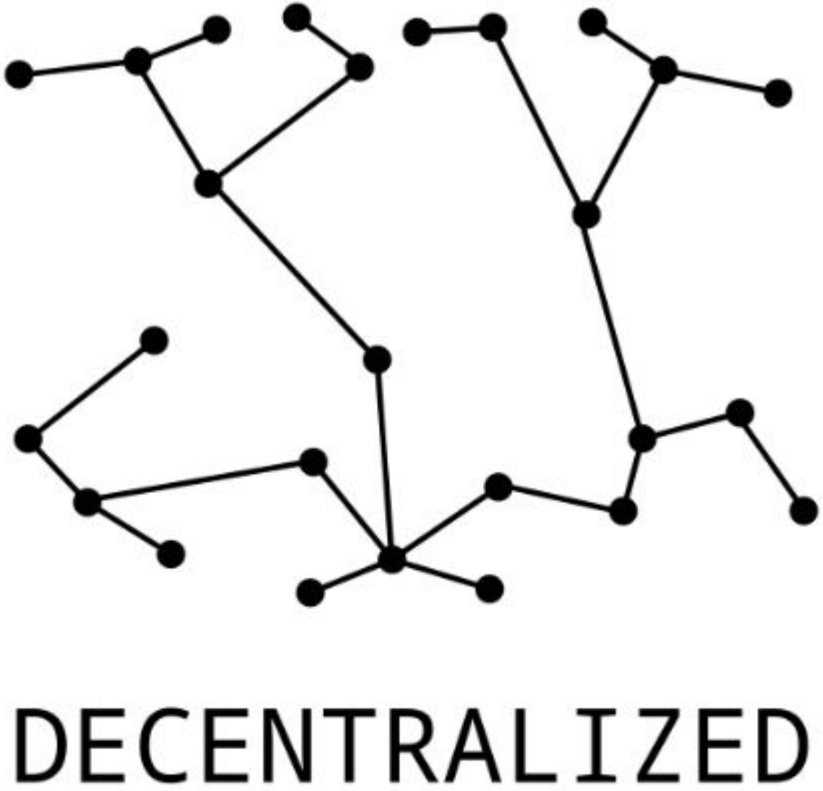
m1, m2, m3, m4, …

m1, m2, m3, m4, …

m1, m2, m3, m4, …

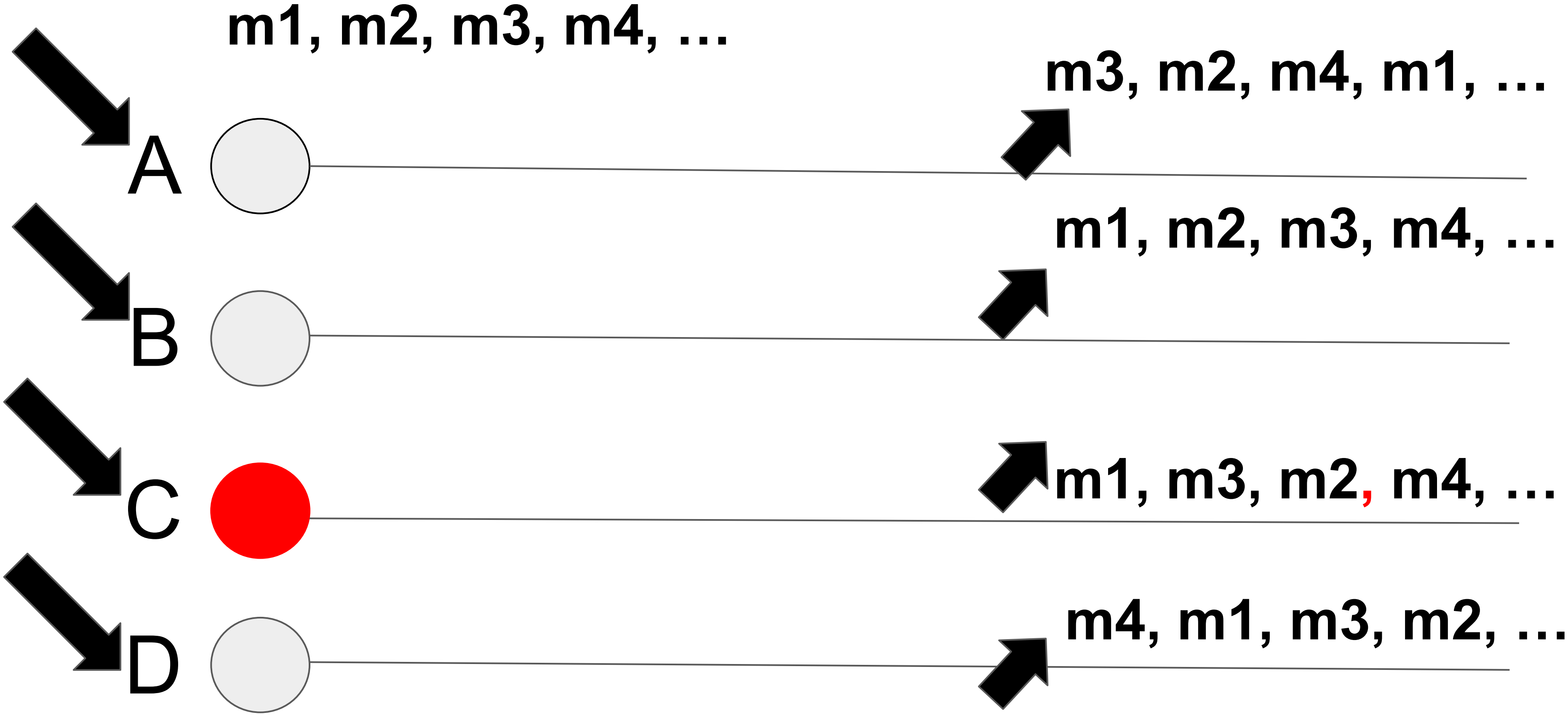
m1, m3, m2, m4, …

m1, m2, m3, m4, …



Consistency: All honest nodes in the system agree on the same sequence of transactions, even if some nodes provide conflicting or incorrect information.

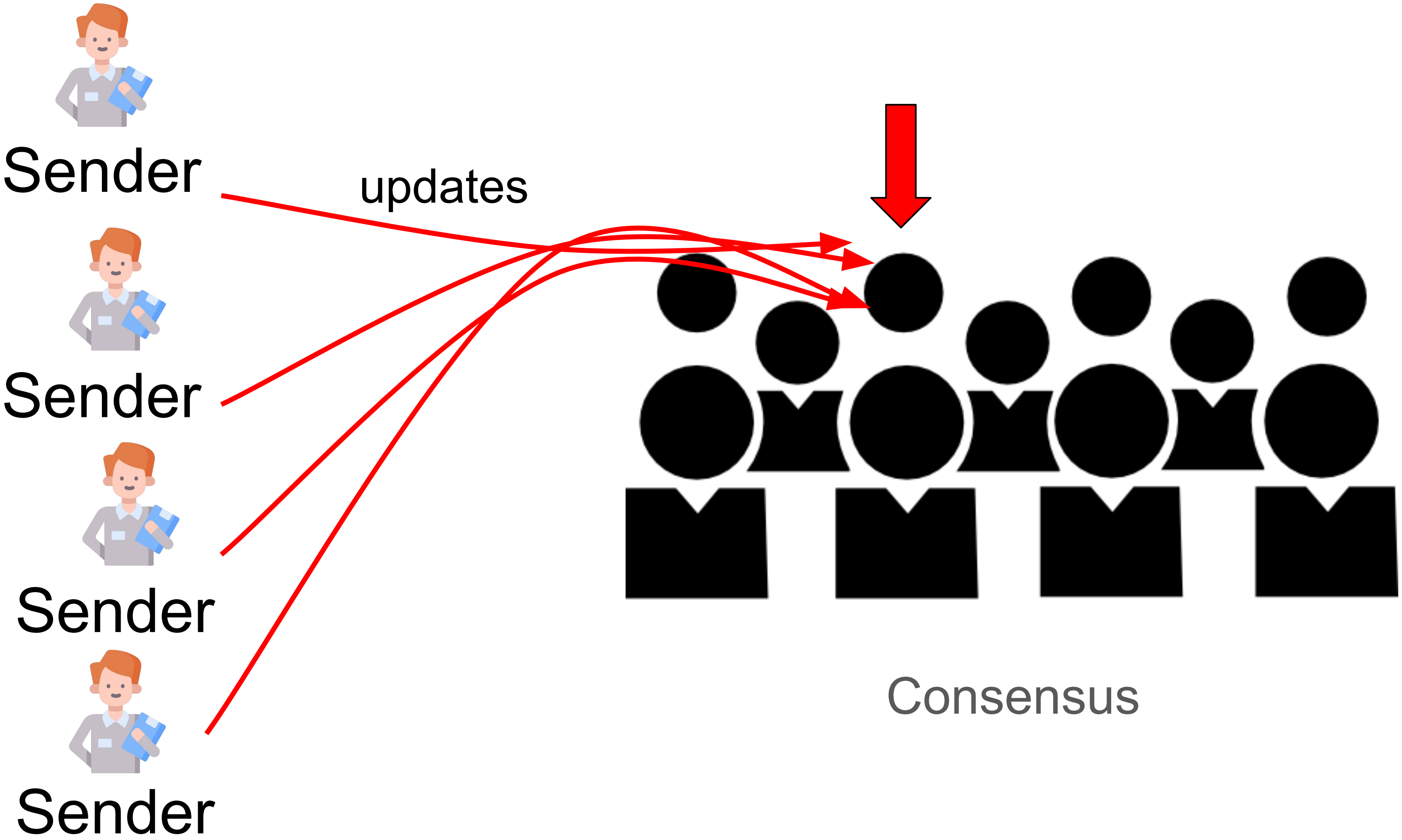
Fault Tolerance: BFT systems can tolerate up to (n-1)/3 faulty nodes in a network of n nodes, ensuring system availability and correctness despite failures.

m1, m2, m3, m4, …
A
B
C
D
m3, m2, m4, m1, …
m1, m2, m3, m4, …
m1, m3, m2, m4, …
m4, m1, m3, m2, …

Sequence 1: Update Email = “12345@gmail”

Sequence 2: Update Email = “6789@gmail”

The database will update seq 2 first and then seq 1



Sender

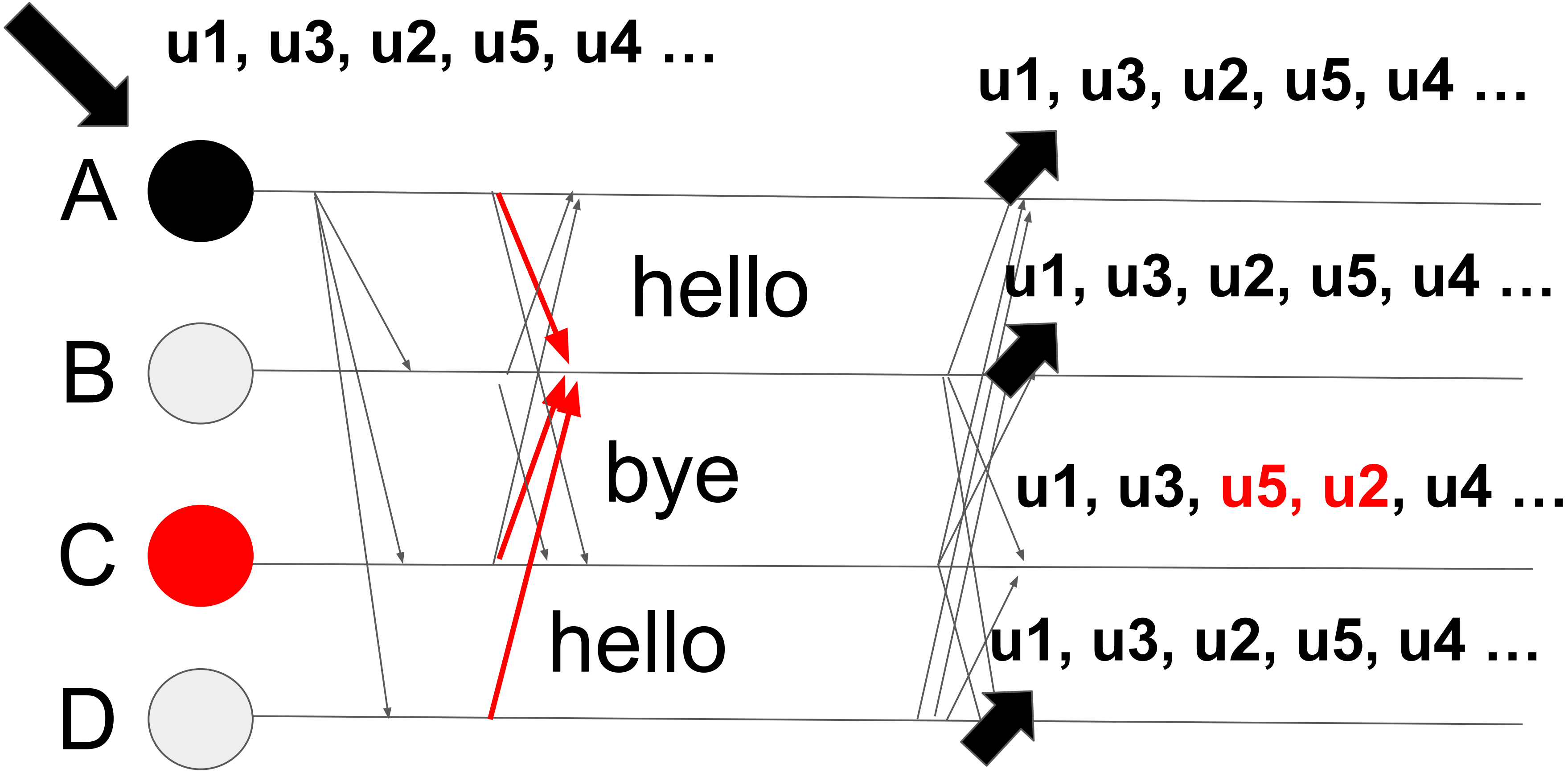
updates

Sender

Sender

Sender

Consensus



u1, u3, u2, u5, u4 …

A

B

C

D

hello

bye

hello

u1, u3, u2, u5, u4 …

u1, u3, u2, u5, u4 …

u1, u3, u5, u2, u4 …

u1, u3, u2, u5, u4 …

A simple example to conclude the workflow:

Step1: I send message to the leader.

Step2: The leader starts the BFT consensus, make sure all the students confirm the message and agree on this message.

Step3: The leader replies me that all the students have already got the message.

Step4: Done! I will start to send a new message to the leader to start a new consensus.

Why we need BFT?

1, Improve data consistency.

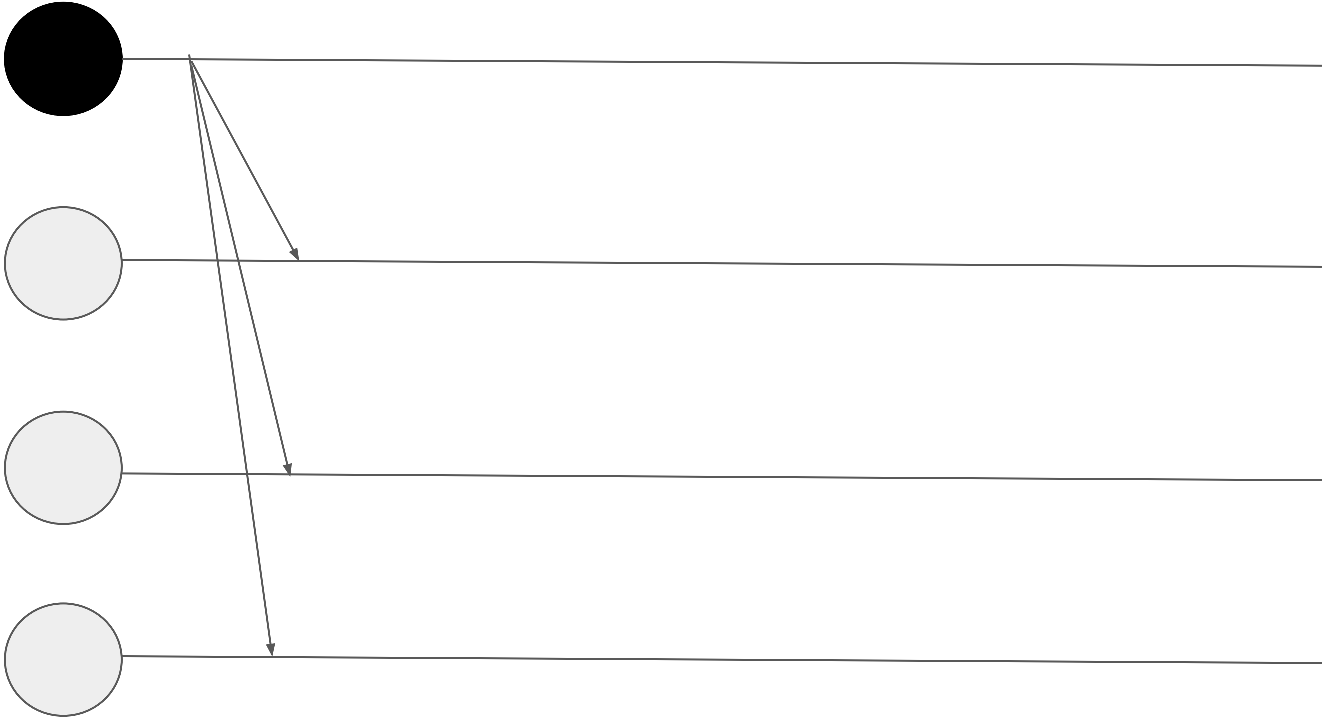
2, Improve system availability.

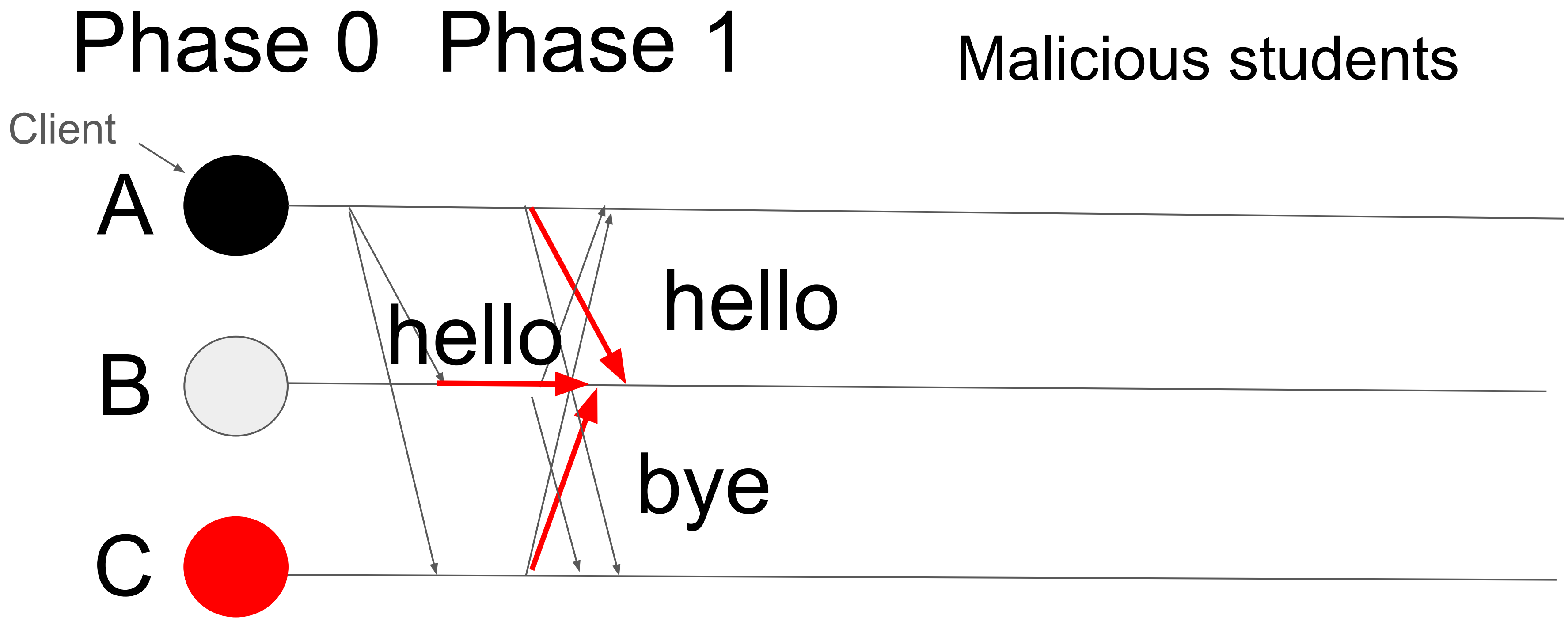
3, tolerating single point of failure

4, tolerating malicious attacks

5, make sure all the requests are in same sequence (Total order).

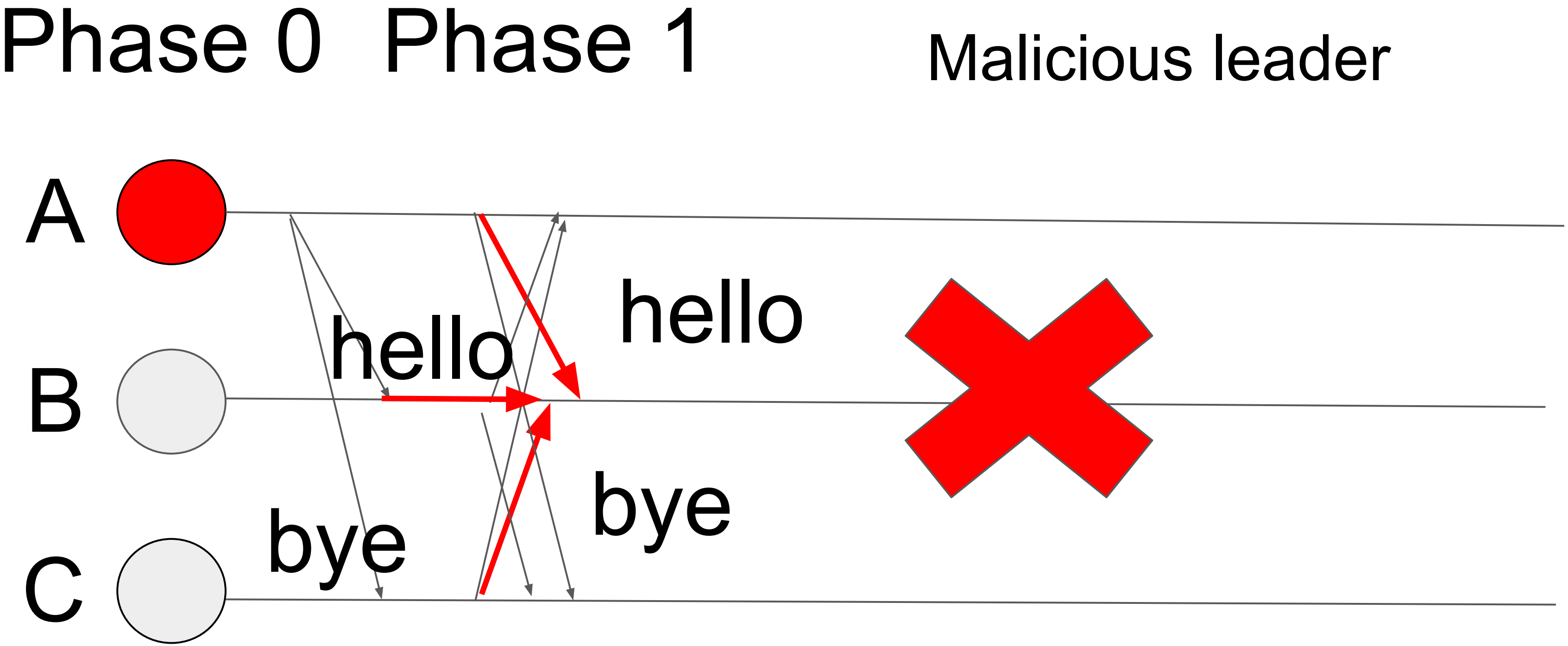
Phase 0





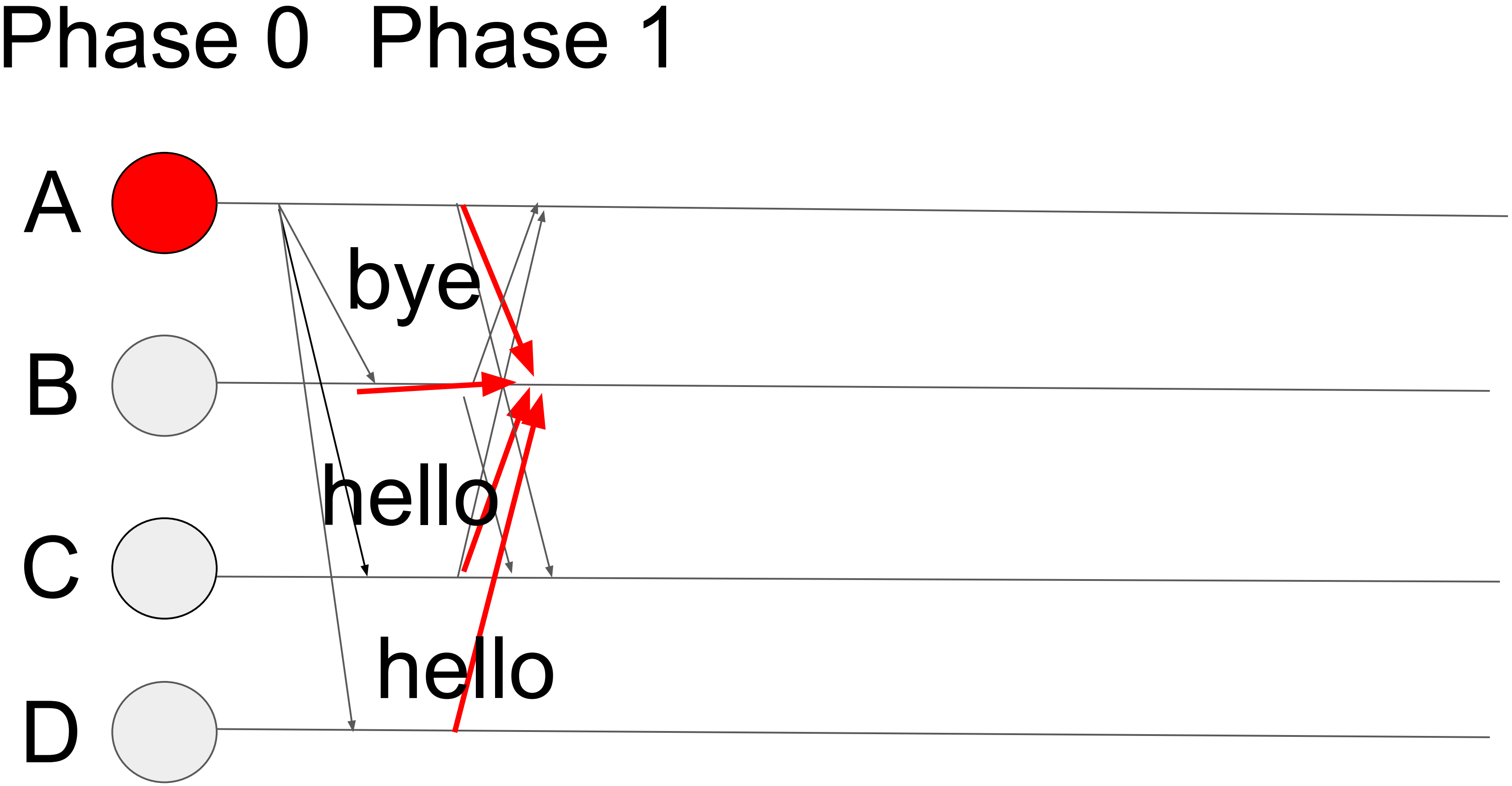
Malicious students

B: (hello), hello, bye



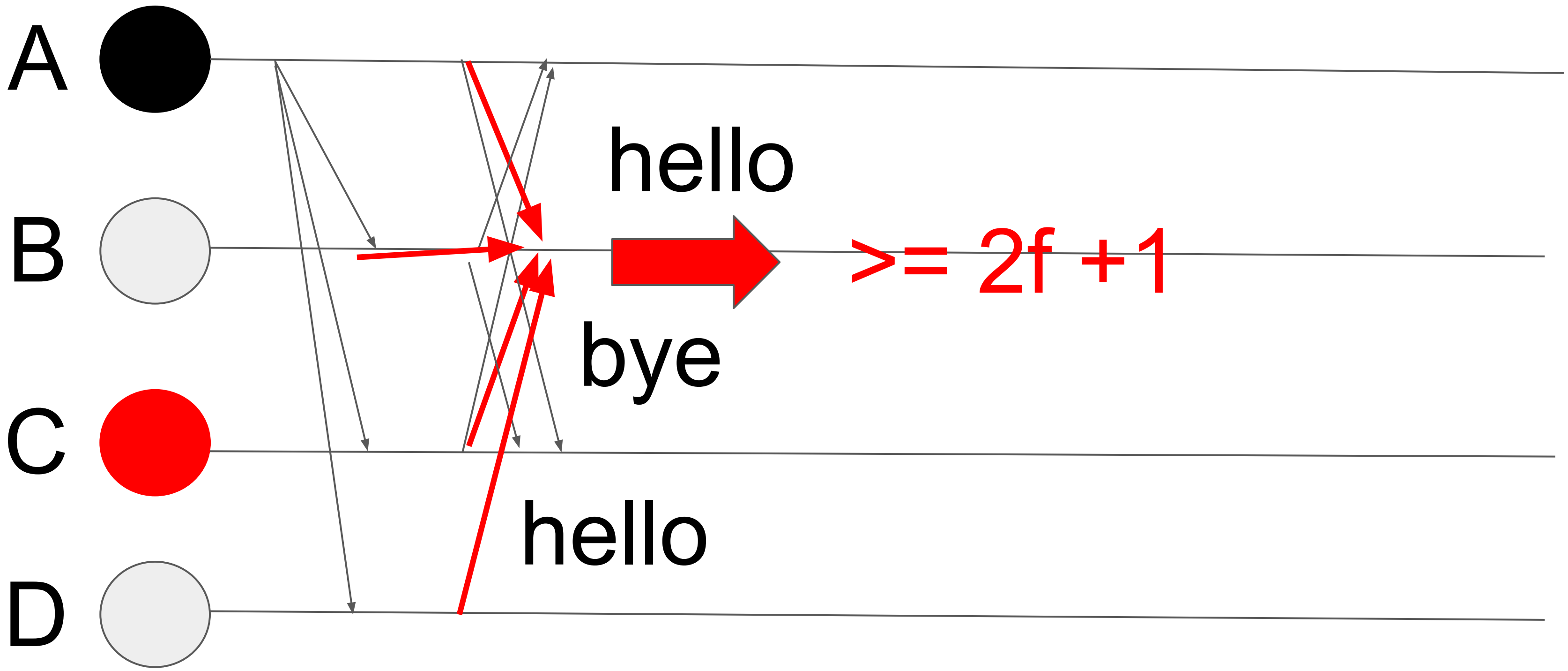
B: (hello), hello, bye

C: (bye), bye, hello



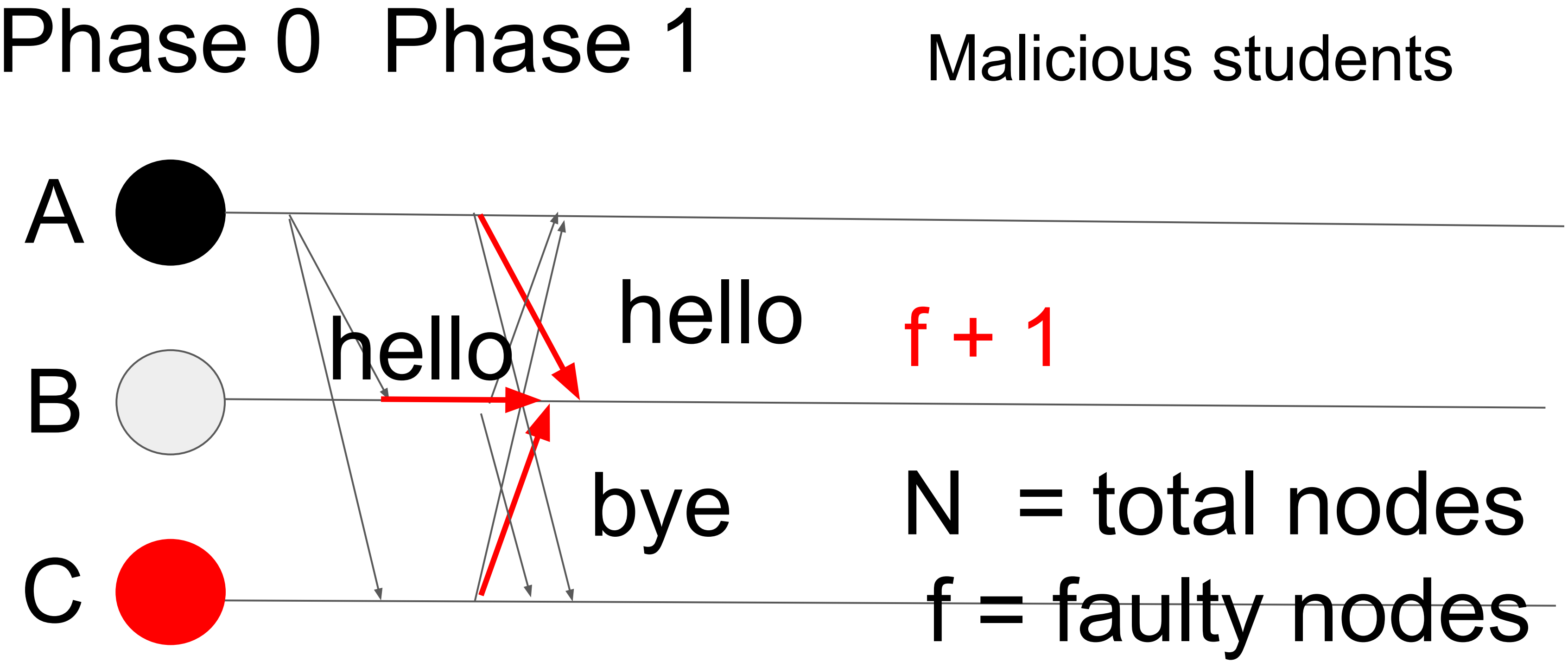
B: (bye), bye, hello, hello

Phase 0 Phase 1



B: (hello), hello, hello, bye

Malicious students

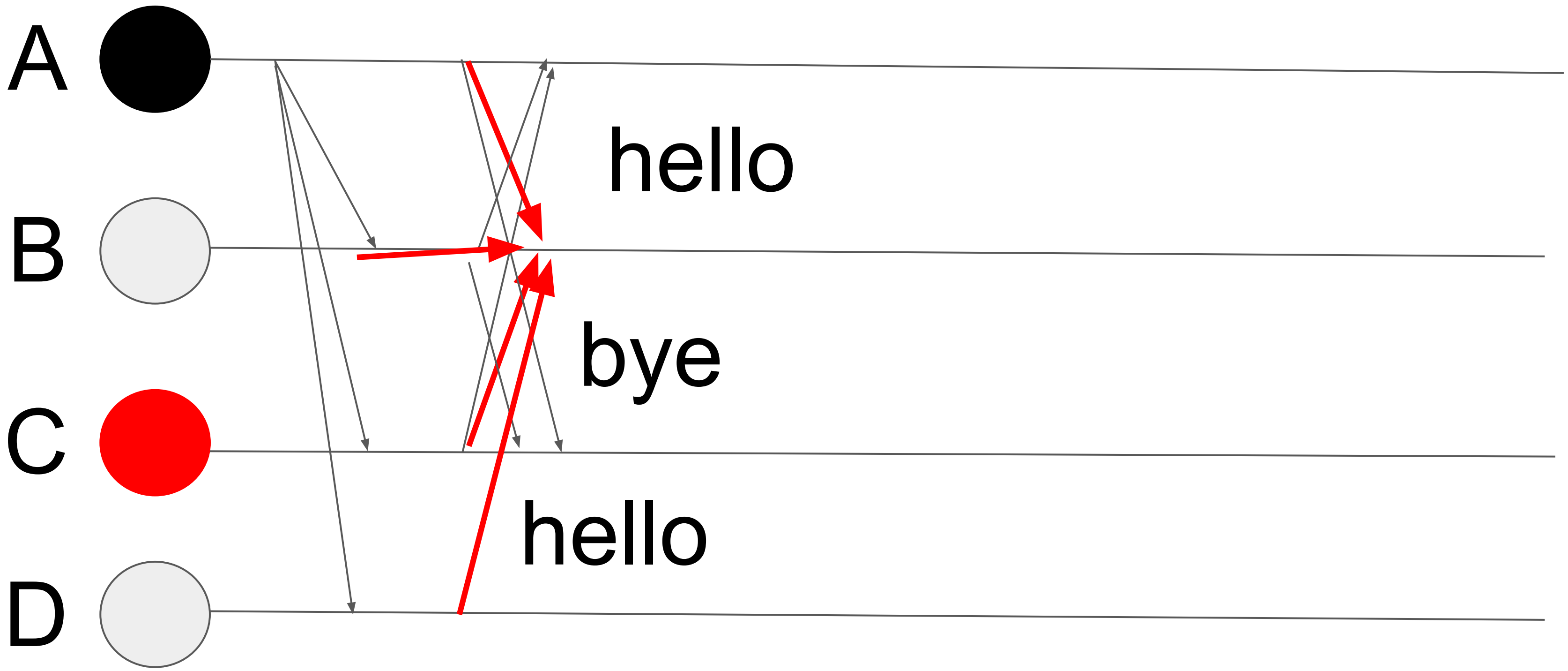


N = total nodes

f = faulty nodes

B: (hello), hello, bye

Phase 0 Phase 1



B: (hello), hello, hello, bye

Why $n >= 3f + 1$?? How to calculate this equation?

$N - f$: correct nodes

f is faulty nodes.

Every nodes must receive $2f +1$ (majority) same messages to make a decision.

$N - f >= 2f + 1$

→ $N >= 3f+1$

4 nodes can tolerate 1

5 nodes can tolerate 1

6 nodes can tolerate 1

7 nodes can tolerate 2

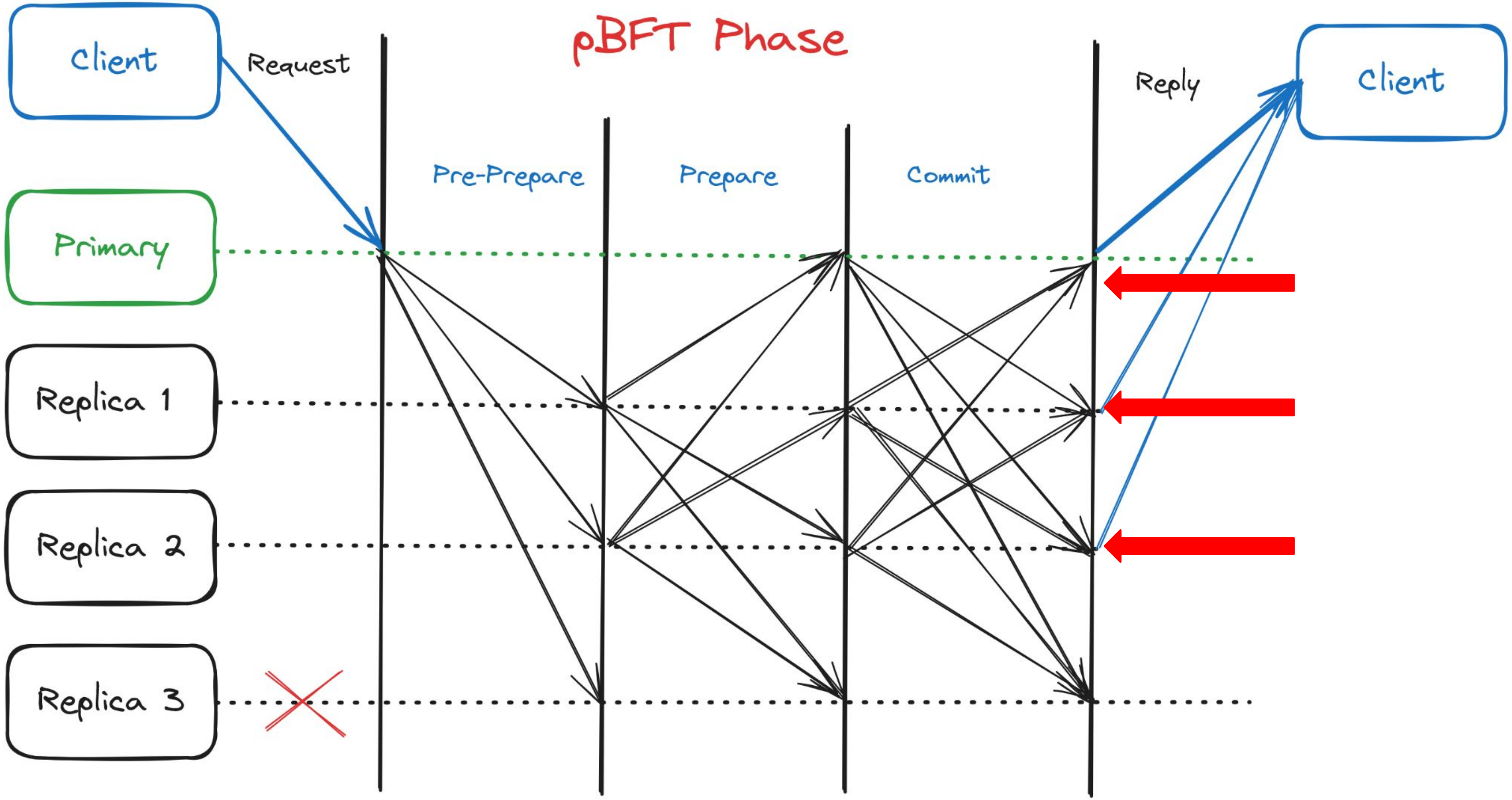
8 nodes can tolerate 2

9 nodes can tolerate 2

10 nodes can tolerate 3

$$n >= 3f + 1$$

Practical Byzantine Fault Tolerance



Financial Transaction Systems

- **Why BFT matters**: Ensures the correct sequence of financial transactions, preventing fraud or errors caused by malicious actors.

Distributed Databases

- **Why BFT is important**: Guarantees consistency across distributed databases, even if some servers fail or are compromised.

Blockchain and Cryptocurrencies

- **Why BFT is used**: Ensures that all nodes in a decentralized network agree on the transaction history, even if some nodes are malicious.

Drawbacks of BFT

Time-Consuming Consensus Process

Scalability Issues

Leader Bottleneck

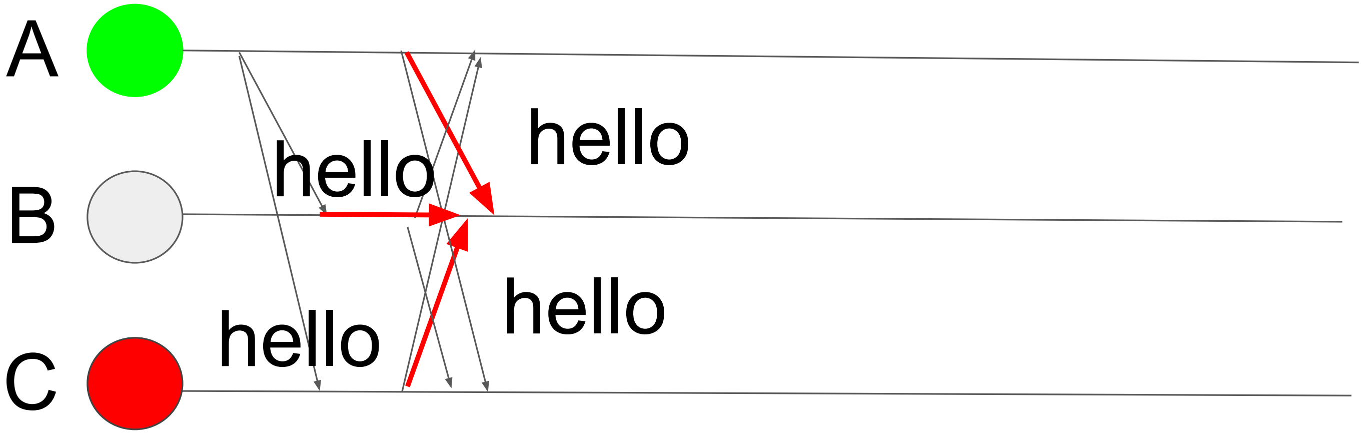
High Latency

Maintenance and Complexity

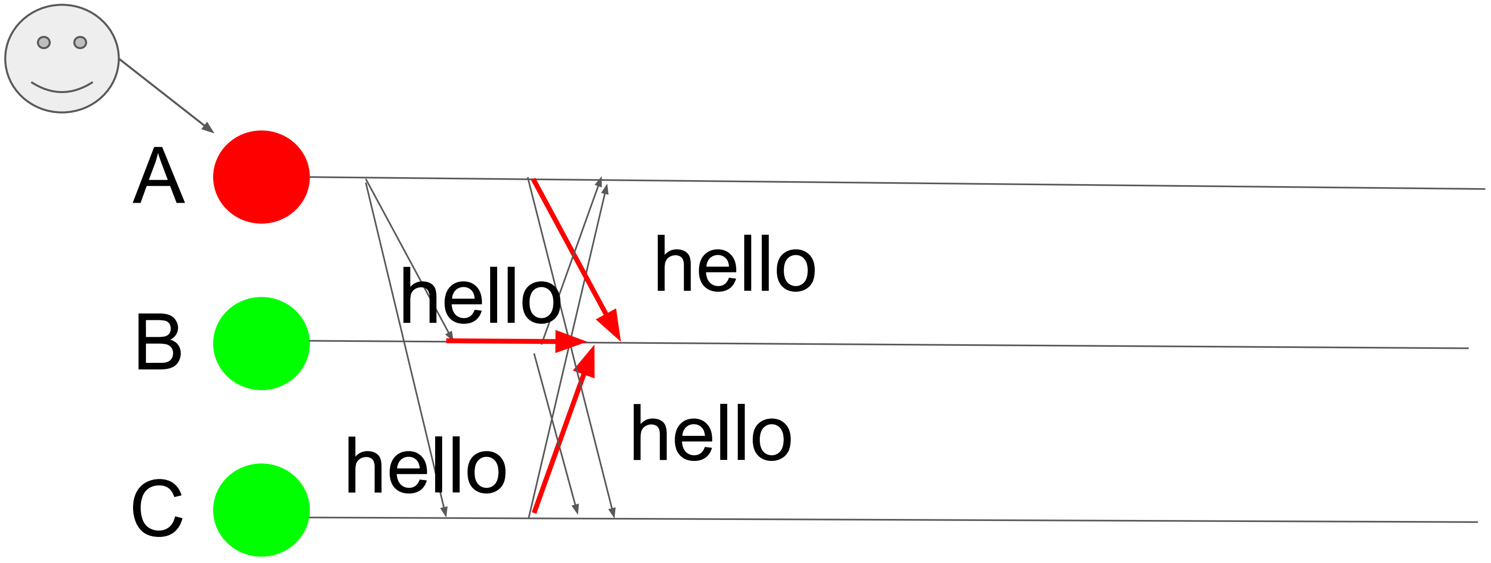
Limited Fault Tolerance Without Increasing Nodes（Only can tolerate 33% malicious nodes）

Vulnerable to Network Delays

If Not too many Byzantine errors: nodes are honest just easy to crash



If leader shutdown, It will be very easy to be detected (the system will get stuck there)



System is secure, just random crash: n >= 2f+1
System is under malicious attack: n >= 3f + 1

Question: Which performance is better?

The performance is big problem of BFT

System is secure, just random crash: n >= 2f+1
System is under malicious attack: n >= 3f + 1

Question: Which performance is better?

The performance is big problem of BFT

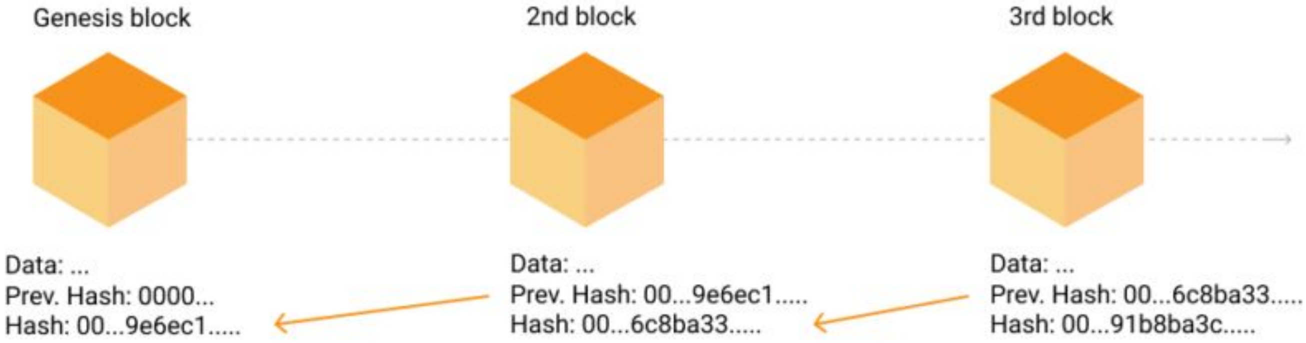
Bitcoin == “Application”

Blockchain == “an Architecture”

https://newhedge.io/bitcoin/node-map

What is a blockchain?

A blockchain is a data structure where information is stored in blocks and cryptographically chained together.



Question:

Features of the blockchain application？ Why need it?

CSC 116 DDoS Attacks

DDoS (Distributed Denial of Service)

Case study

Have you ever tried to visit a website, but it was extremely slow or completely down? It might have been under a DDoS attack.

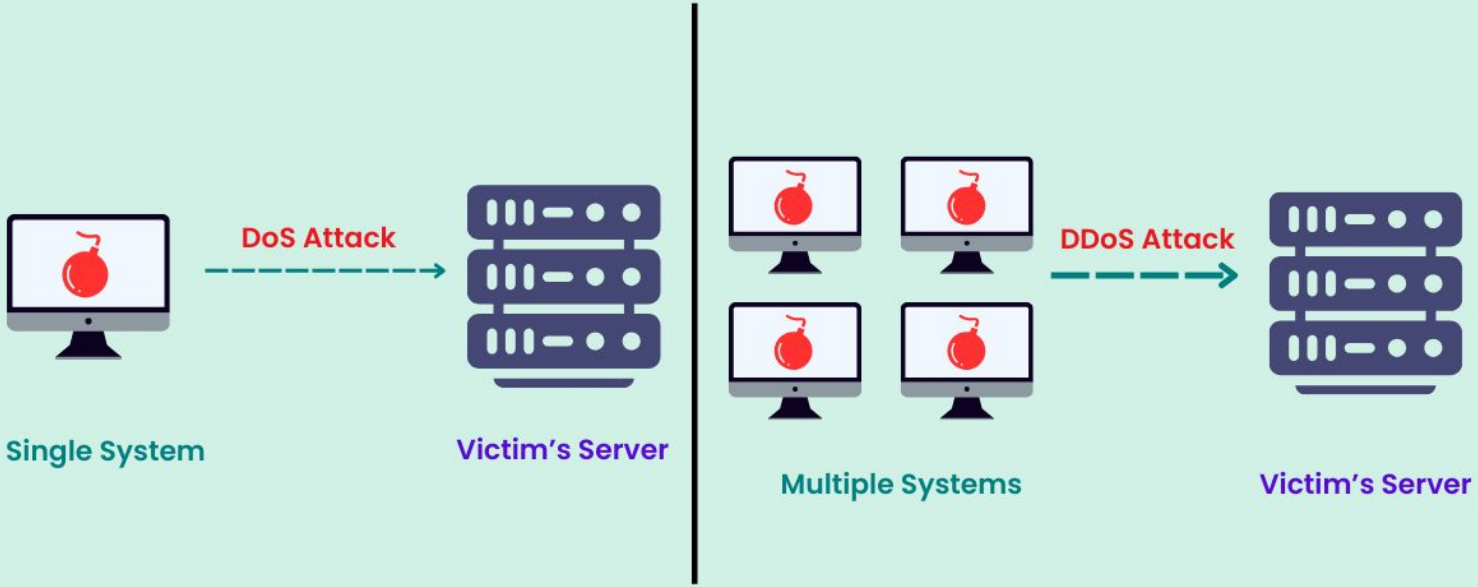
Definition of DoS

A cyber attack that floods a website or server with fake traffic to make it unavailable.

Difference between **DoS vs. DDoS**:

- **DoS (Denial of Service)**: A single attacker floods a target with requests.
- **DDoS (Distributed Denial of Service)**: Multiple devices (botnets) are used to overwhelm the target.

DoS vs DDoS Attacks



Why Do Hackers Launch DDoS Attacks?

Solutions

Enable Rate Limiting & CAPTCHAs

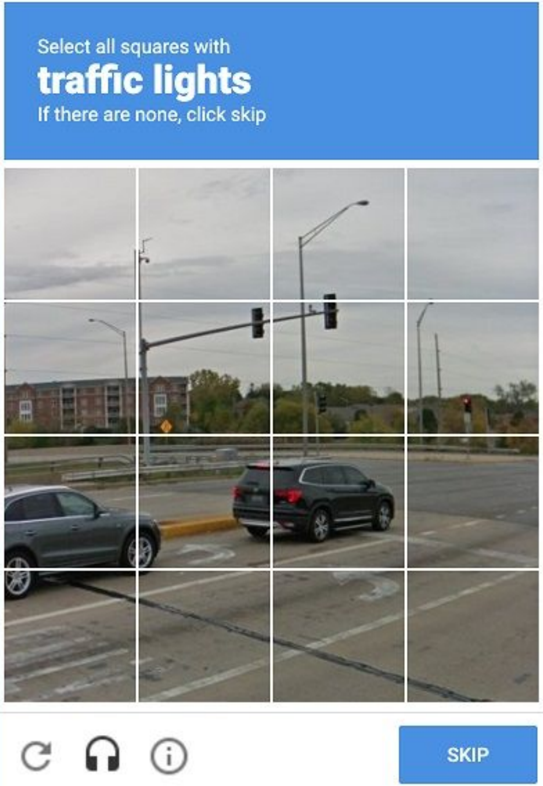
- If you run a personal website (e.g., a school project), enable:
  - **Rate limiting** (limits the number of requests per IP).
  - **CAPTCHA verification** to block bots.
  - **Web Application Firewall (WAF)** (Cloudflare, AWS Shield, etc.).

Monitor Traffic for Anomalies

- Use tools like **Google Analytics, AWStats**, or **UptimeRobot** to check for **sudden spikes in traffic**.
- If you notice **abnormal behavior**, temporarily **block suspicious IPs**.
-

Use Cloud-Based DDoS Protection

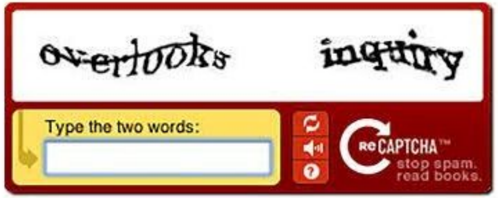
- Services like **Cloudflare Free Plan**, **Google Shield**, or **AWS Free Tier** offer basic **DDoS mitigation**.
- They provide **rate limiting**, **IP filtering**, and **traffic distribution**.



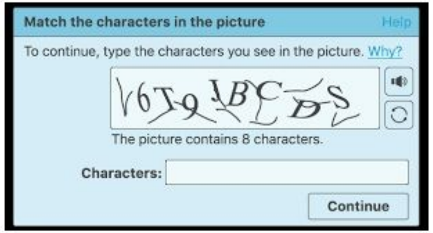
Select all squares with

traffic lights

If there are none, click skip



Type the two words:

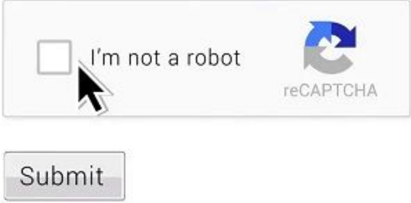


Match the characters in the picture

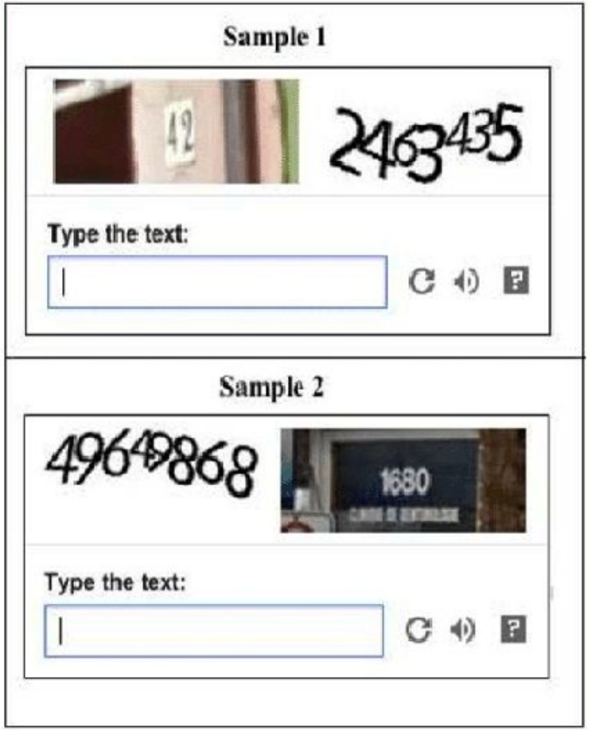
To continue, type the characters you see in the picture. Why?

The picture contains 8 characters.

Characters:



□ I'm not a robot



Sample 1

Type the text:

Sample 2

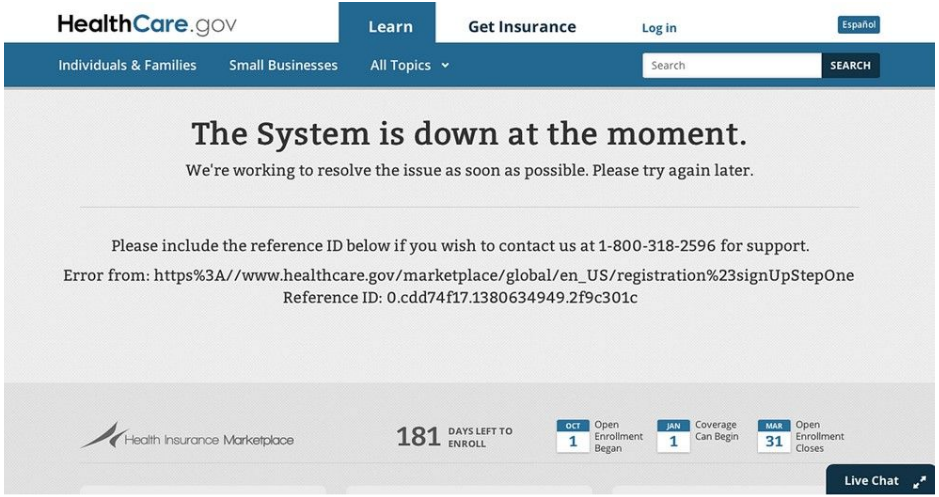
Type the text:

Next Important Topic:

The importance of the Server Performance to handle requests.

Good Server

Bad Server



The System is down at the moment.

We're working to resolve the issue as soon as possible. Please try again later.

Please include the reference ID below if you wish to contact us at 1-800-318-2596 for support.

Error from: https%3A//www.healthcare.gov/marketplace/global/en_US/registration%23signUpStepOne
Reference ID: 0.cdd74f17.1380634949.2f9c301c

Health Insurance Marketplace
181 DAYS LEFT TO ENROLL
OCT 1 Open Enrollment Began
JAN 1 Coverage Can Begin
MAR 31 Open Enrollment Closes
Live Chat

Server Performance

If the webpage is requesting data from a **self-hosted server**, the request rate depends on:

- CPU and RAM capacity of the server.
- Use of optimization tools like **Nginx / Apache / Load Balancer**.
- Concurrency handling capacity:
    - **Nginx** can handle **thousands of QPS (Queries Per Second)**.
    - **Flask/Django (single-threaded)** servers may handle **tens to hundreds of QPS**.

But it is not enough in Black Friday!!

SALE
30%
50%
SALE
SALE
50%
SALE
SALE
SALE