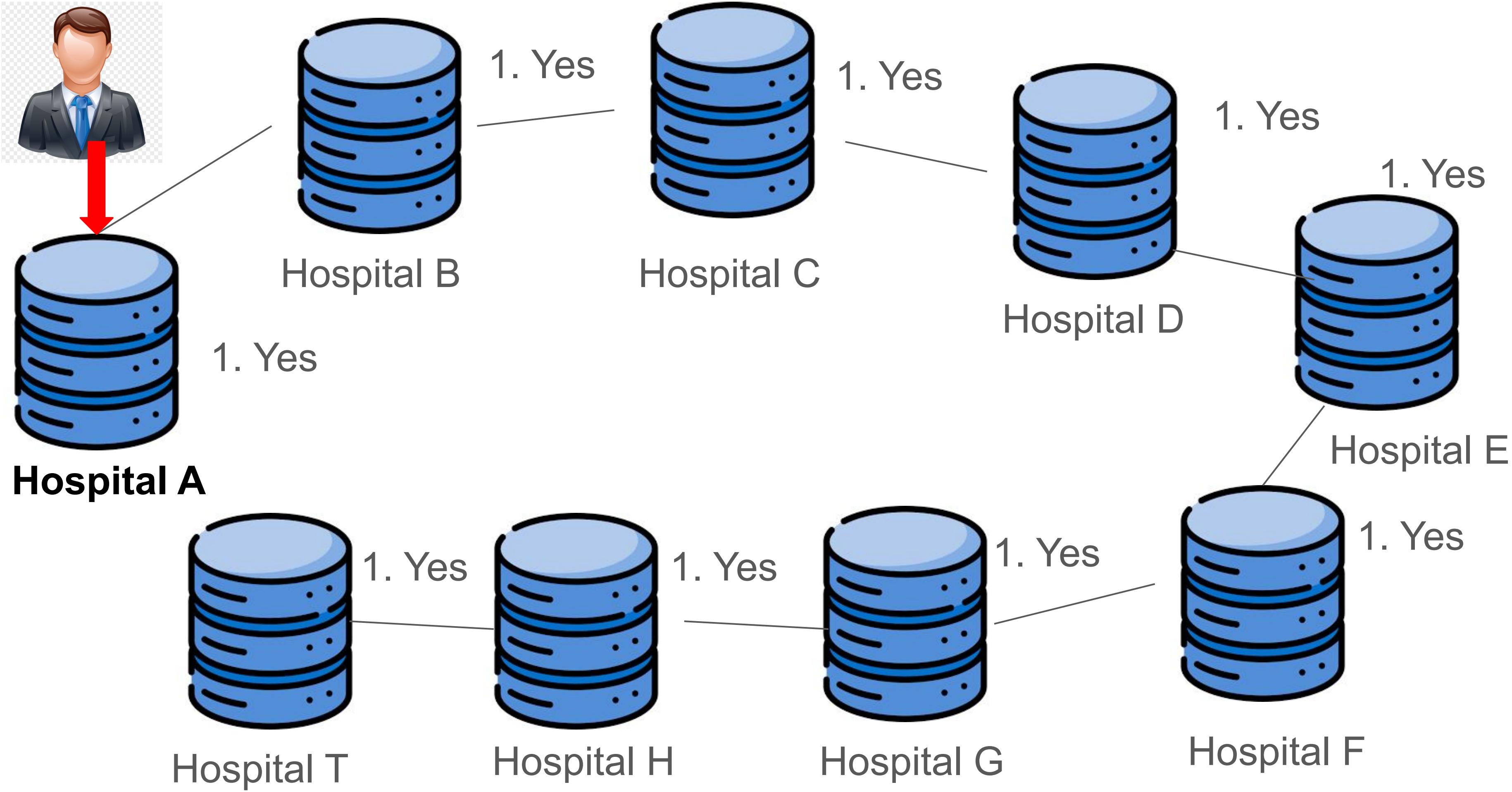
CSC 116 Blockchain



Hospital A

1. Yes

Hospital B

1. Yes

Hospital C

1. Yes

Hospital D

1. Yes

Hospital E

1. Yes

Hospital F

1. Yes

Hospital G

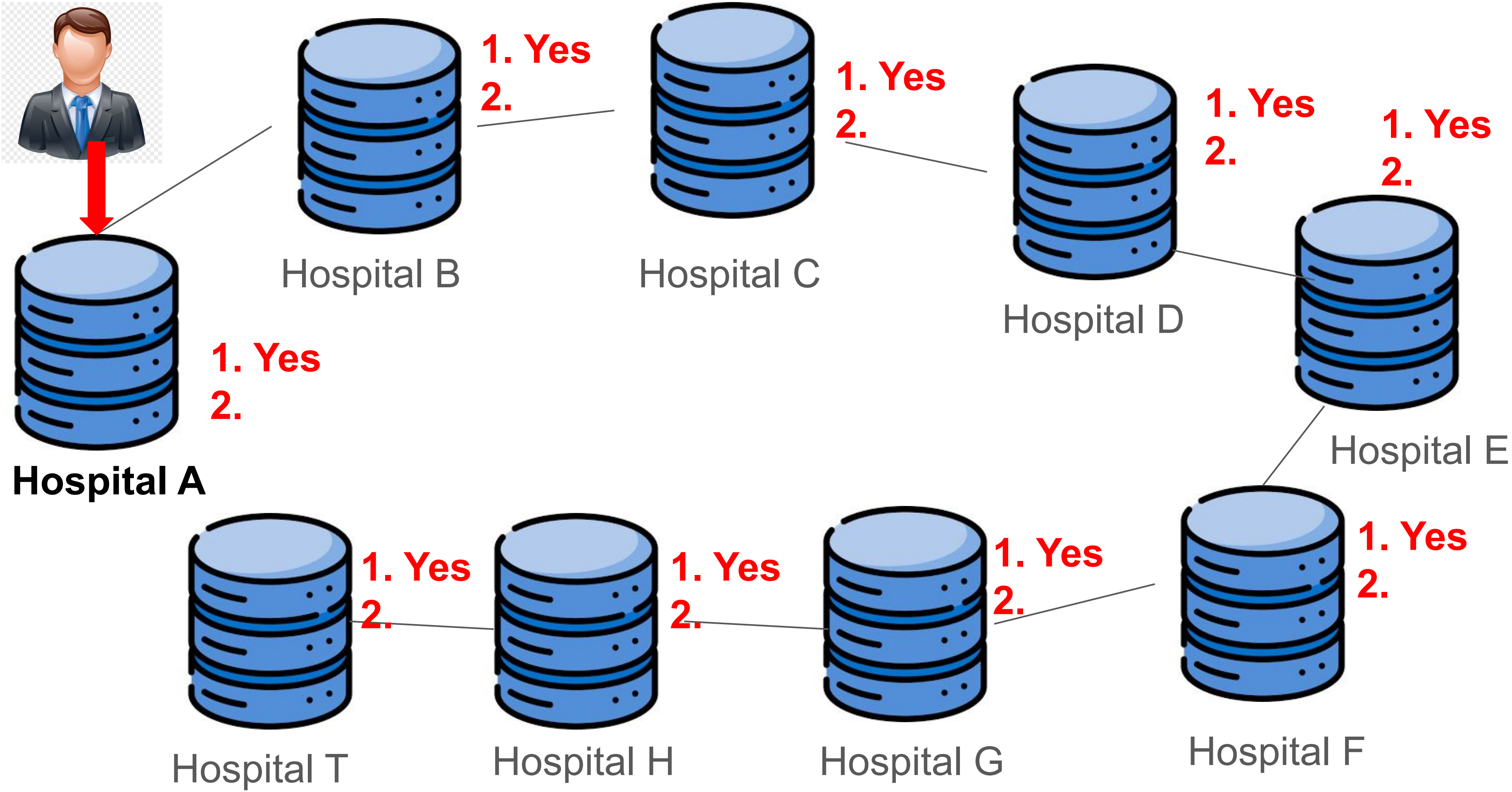
1. Yes

Hospital H

1. Yes

Hospital T

1. Yes



1. Yes
2.

Hospital A

1. Yes
2.

Hospital B

1. Yes
2.

Hospital C

1. Yes
2.

Hospital D

1. Yes
2.

Hospital E

1. Yes
2.

Hospital F

1. Yes
2.

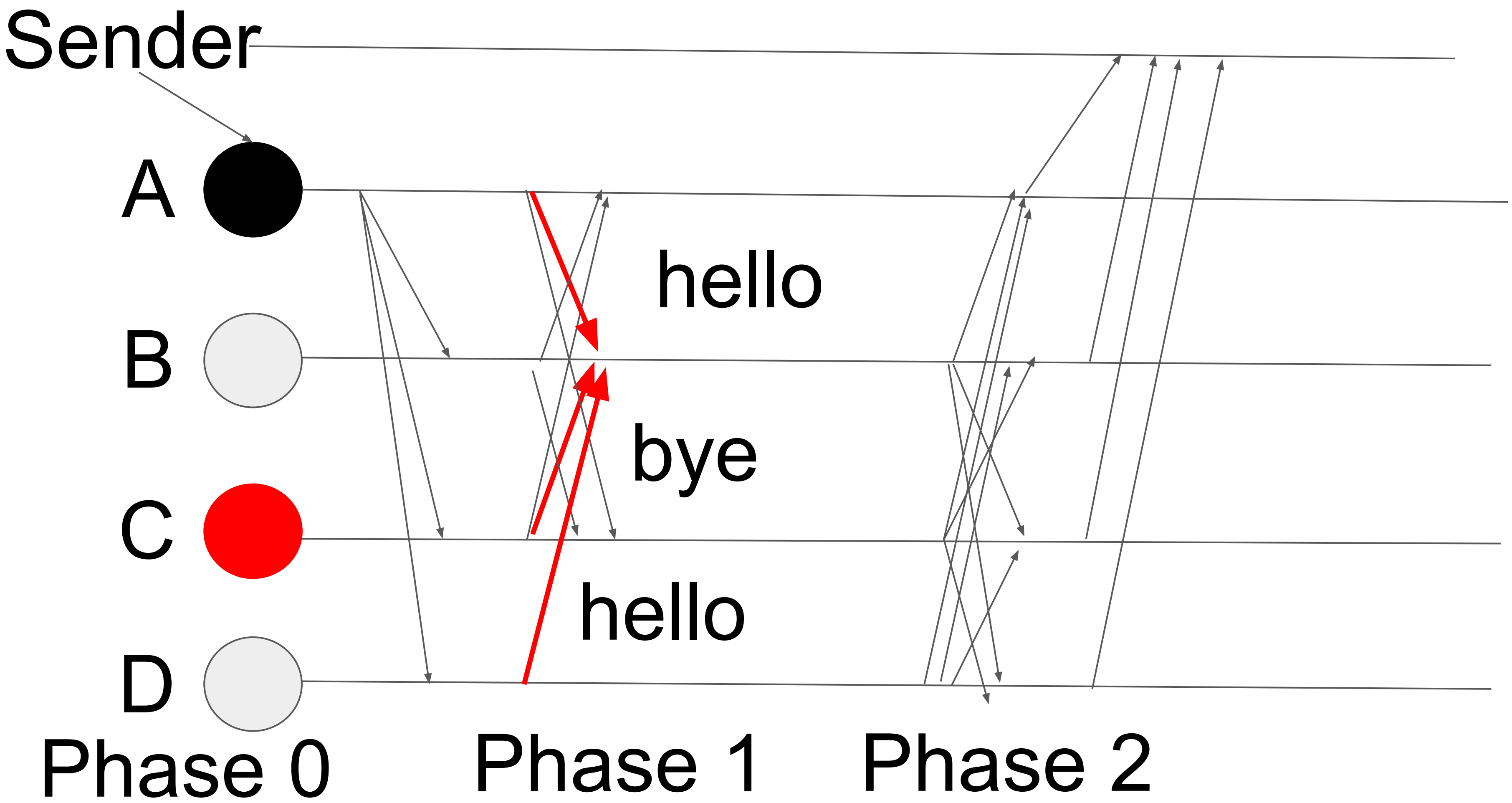
Hospital G

1. Yes
2.

Hospital H

1. Yes
2.

Hospital T


Sender
A
B
C
D
hello
bye
hello
Phase 0
Phase 1
Phase 2

Phase 0: send messages to everyone

Phase 1: ensuring that your messages that you received are correct: You need to select the majority ones.

Phase 2: after you decided, you need to tell your final decision to everyone, so everyone will store the data in their local database, and reply to sender. So sender will send a new message (sender is waiting, leader is waiting your reply as well)

Why we need BFT?

To make agreement with all the nodes. So all the nodes will do the same order.

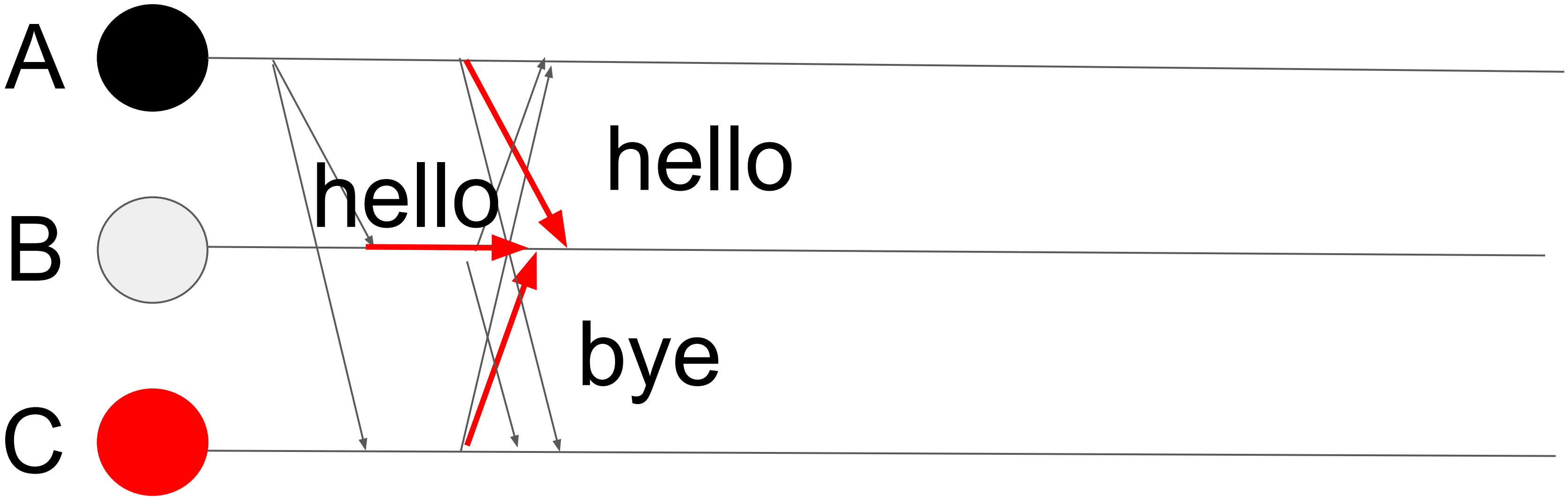
Which means all the nodes will store the messages in same order (total order & totality).

Why need leader? Why can not leader just broadcast messages in a strict order to all of you?

Network delay:
You will receive order 2 first, and then order 1 because of the network delay or attack.

Malicious students

Phase 0 Phase 1



A

B

C

hello

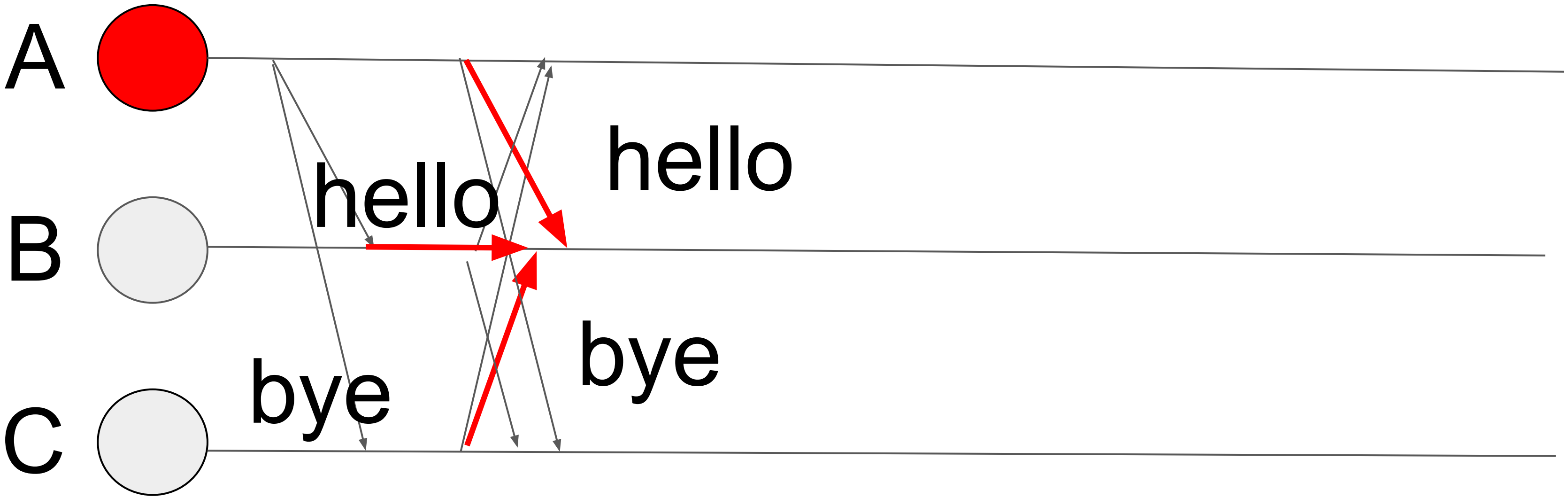
hello

bye

B: (hello), hello, bye

Malicious leader

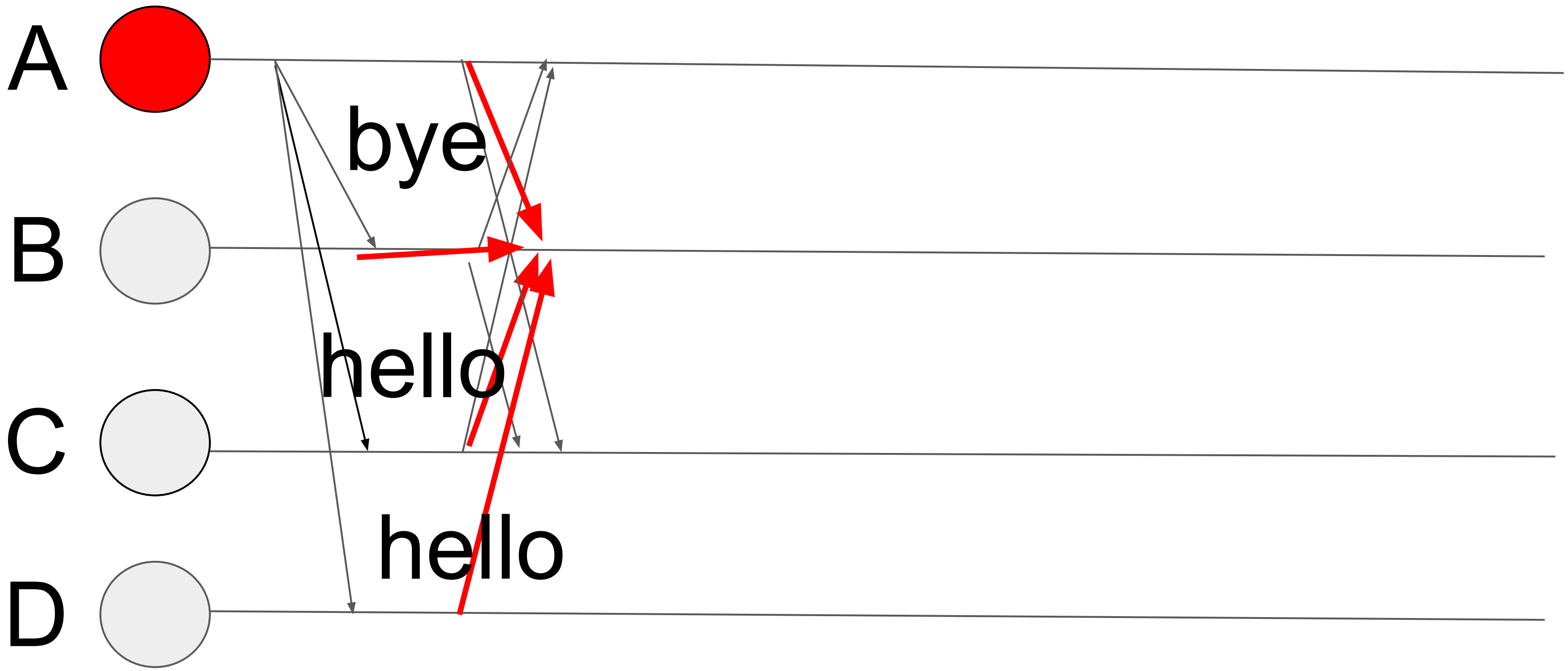
Phase 0 Phase 1



B: (hello), hello, bye

C: (bye), bye, hello

Phase 0 Phase 1



A

B

C

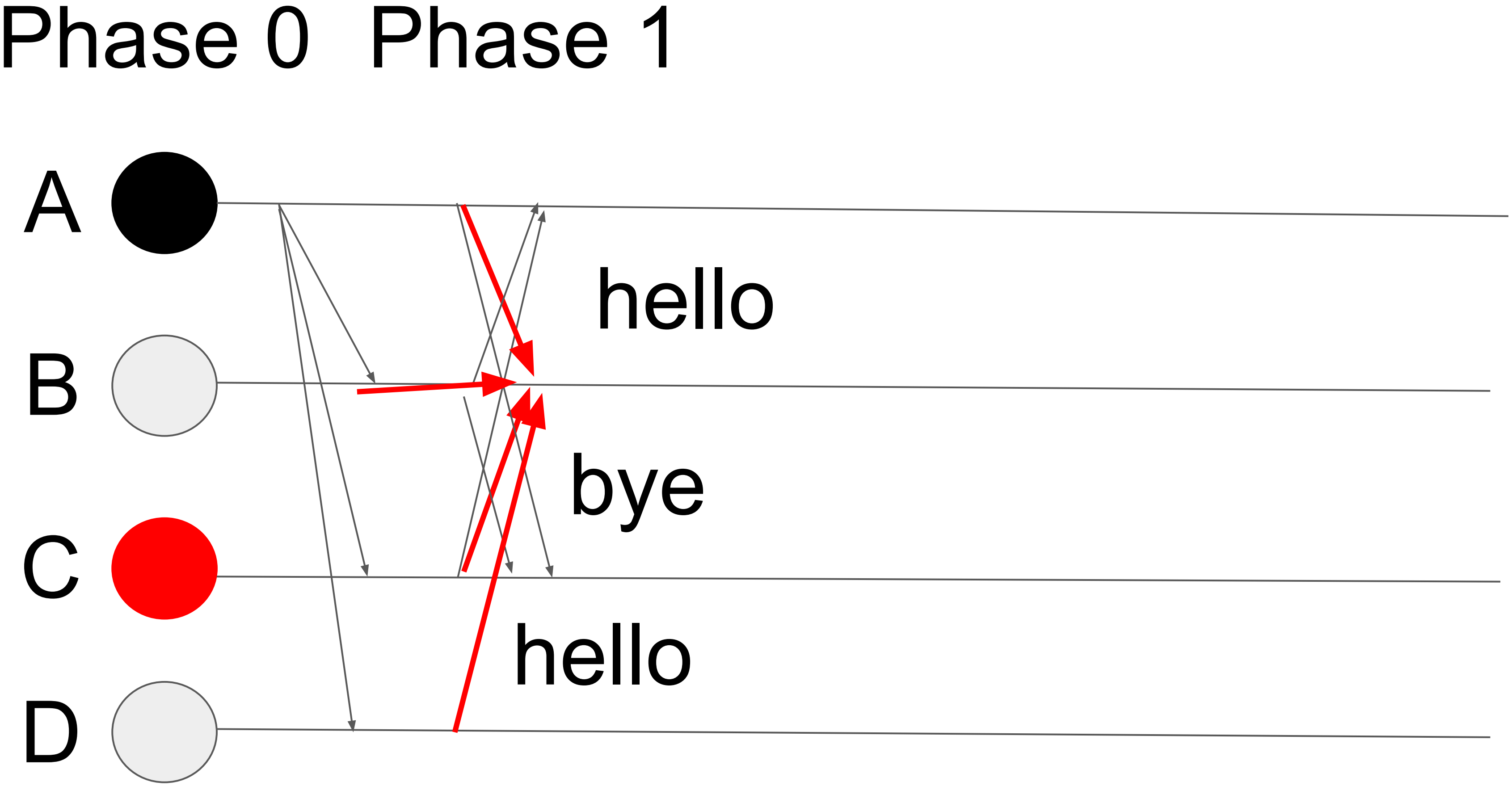
D

bye

hello

hello

B: (bye), bye, hello, hello



B: (hello), hello, hello, bye

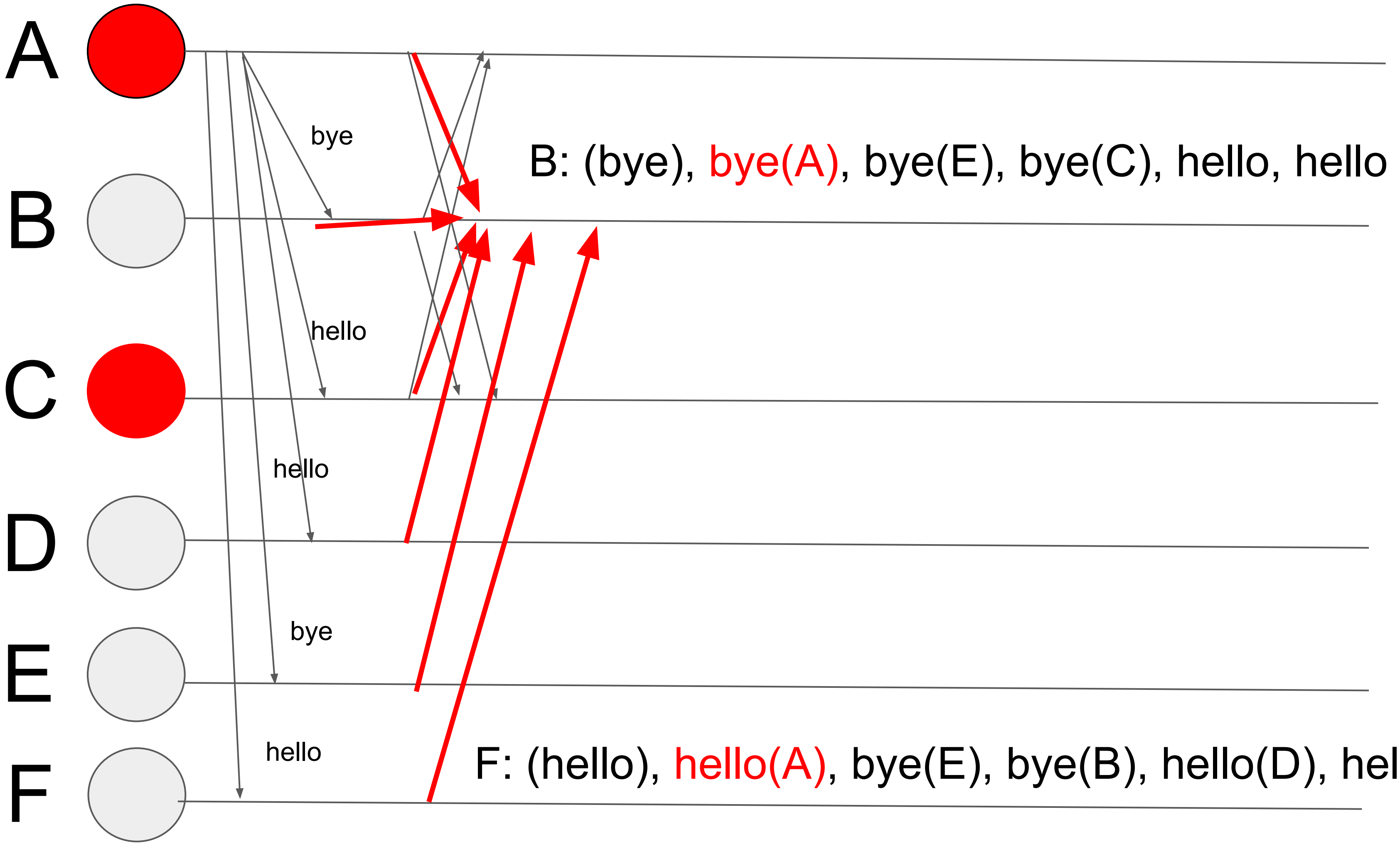
n: total nodes

f: total number of malicious nodes

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

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

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



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

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

4 nodes can tolerate 1

5 nodes can tolerate 1

6 nodes can tolerate 1

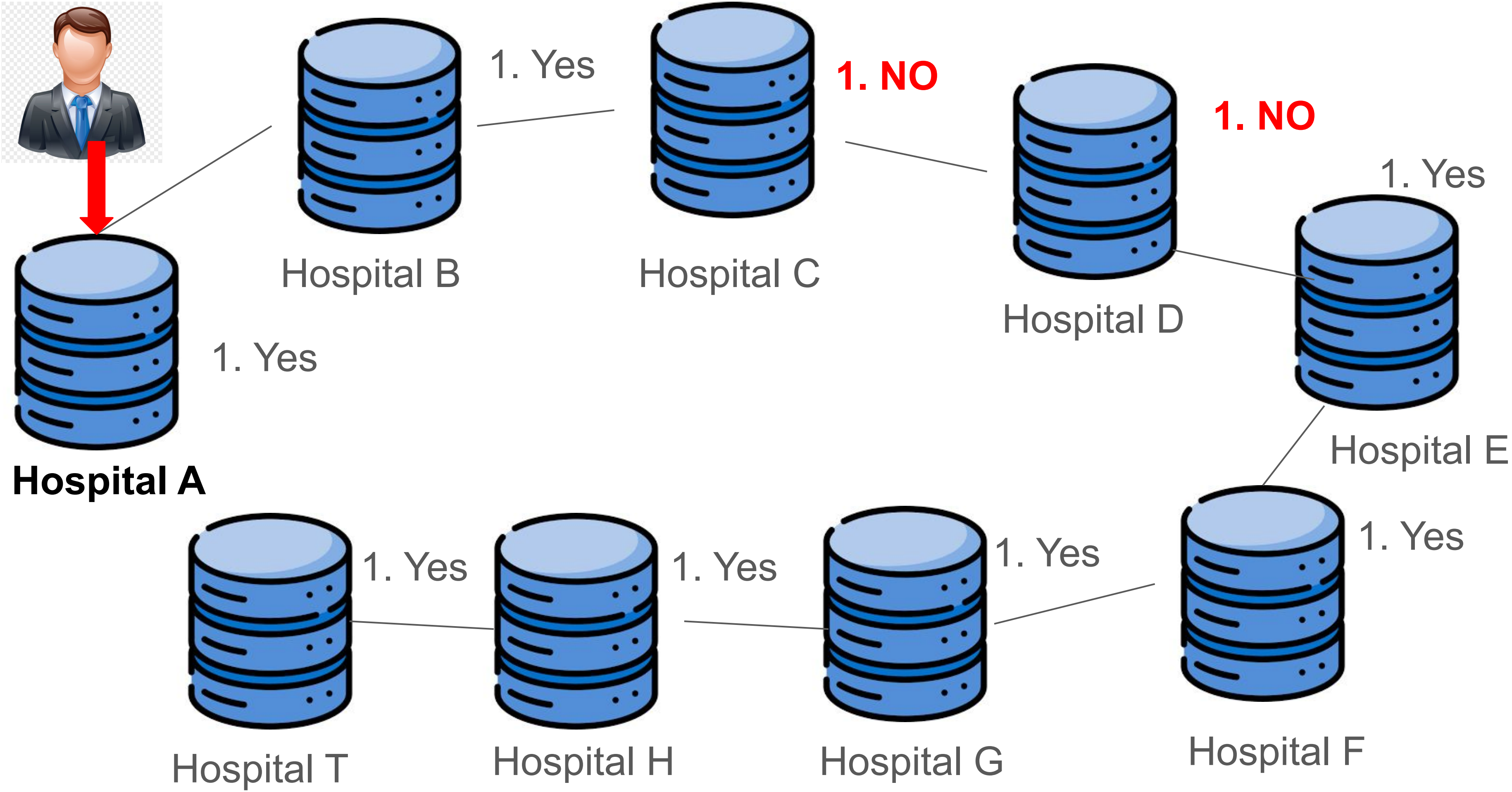
7 nodes can tolerate 2

8 nodes can tolerate 2

9 nodes can tolerate 2

10 nodes can tolerate 3

$$n >= 3f + 1$$



Hospital A

1. Yes

Hospital B

1. Yes

Hospital C

1. NO

Hospital D

1. NO

Hospital E

1. Yes

Hospital F

1. Yes

Hospital G

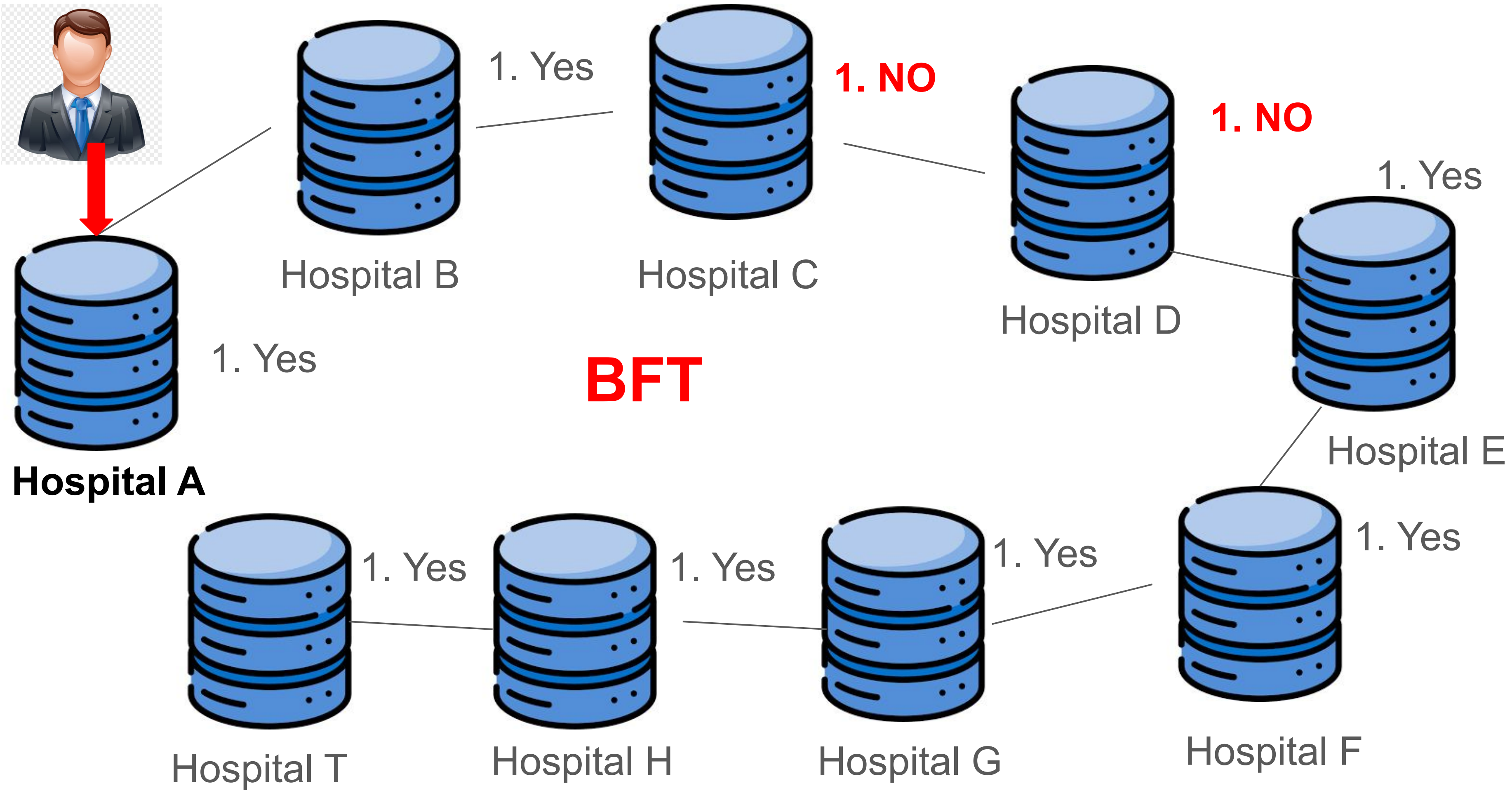
1. Yes

Hospital H

1. Yes

Hospital T

1. Yes



BFT

Hospital A

1. Yes

Hospital B

1. Yes

Hospital C

1. NO

Hospital D

1. NO

Hospital E

1. Yes

Hospital F

1. Yes

Hospital G

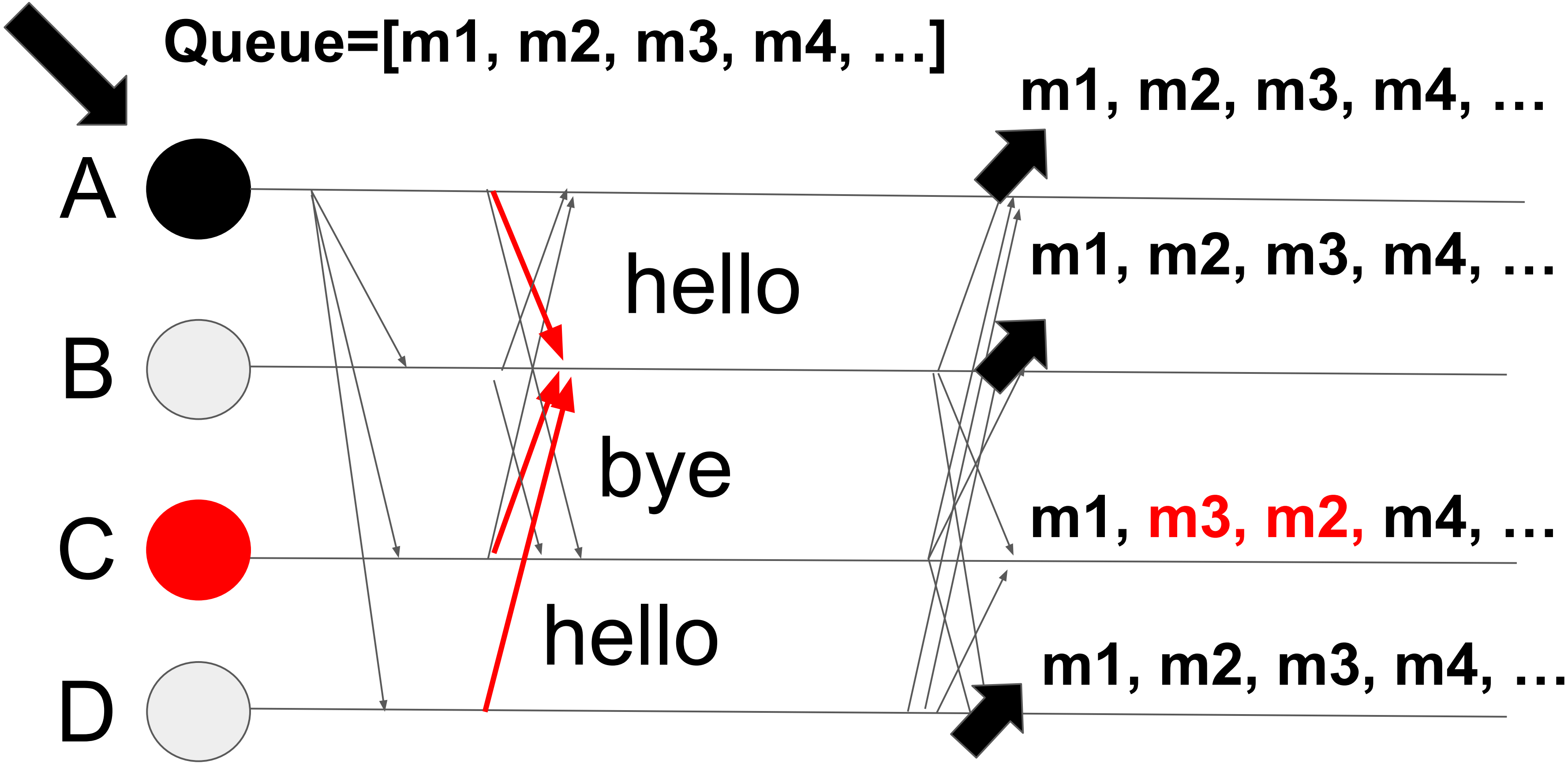
1. Yes

Hospital H

1. Yes

Hospital T

1. Yes



Queue=[m1, m2, m3, m4, …]

A

B

C

D

hello

bye

hello

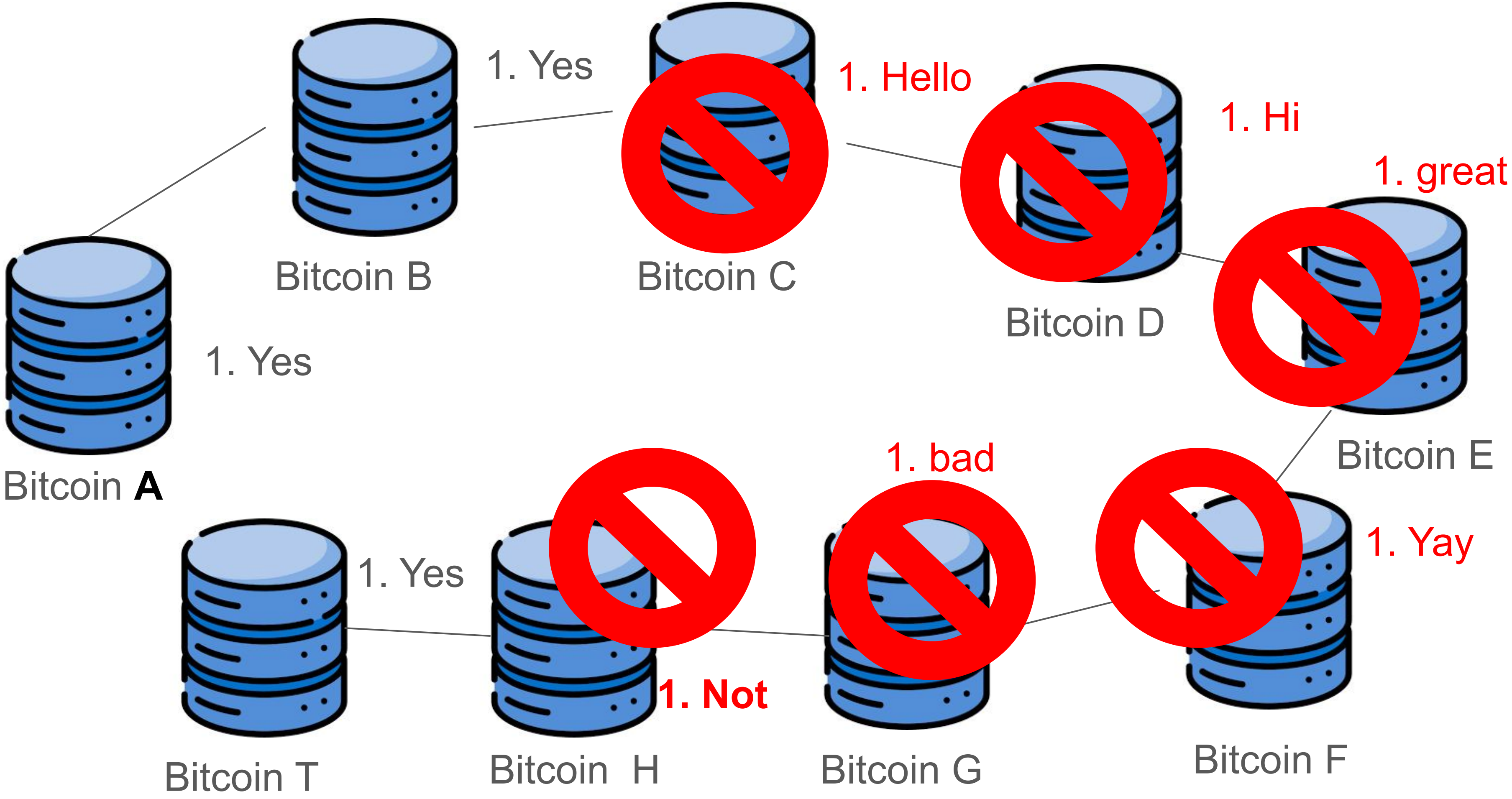
m1, m2, m3, m4, …

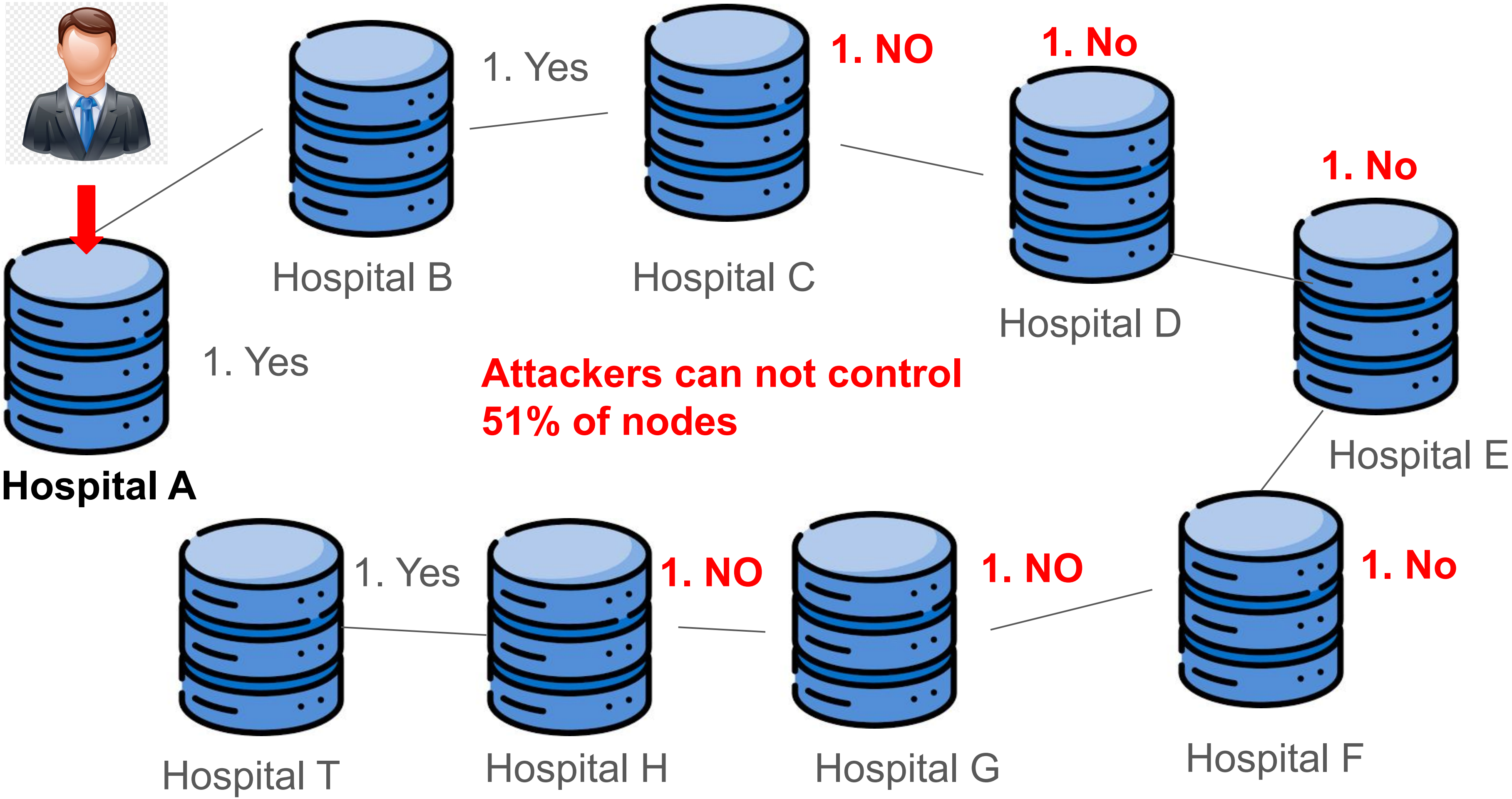
m1, m2, m3, m4, …

m1, m3, m2, m4, …

m1, m2, m3, m4, …

51% Attackers in Bitcoin Blockchain


1. Yes
1. Yes
1. Hello
1. Hi
1. great
Bitcoin A
Bitcoin B
Bitcoin C
Bitcoin D
Bitcoin E
1. Yes
1. bad
1. Yay
1. Not
Bitcoin T
Bitcoin H
Bitcoin G
Bitcoin F



Hospital A

1. Yes

Hospital B

1. Yes

Hospital C

1. NO

Hospital D

1. No

Hospital E

1. No

Hospital F

1. No

Hospital G

1. NO

Hospital H

1. NO

Hospital T

1. Yes

Attackers can not control 51% of nodes

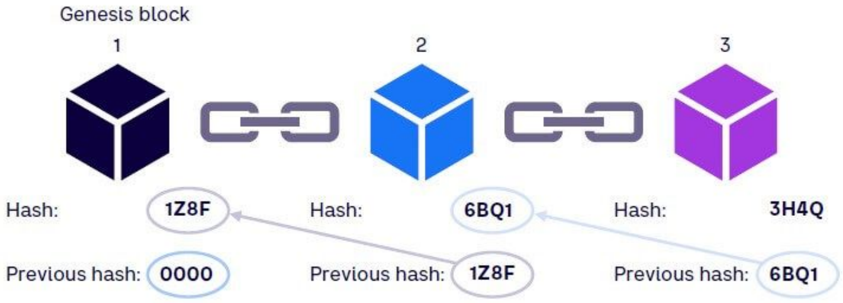
There are so many blockchain nodes: Immutability

The Blockchain has a feature: Immutability. Because the data in the blockchain has so many copies, it is hard to controlled 51% of nodes.

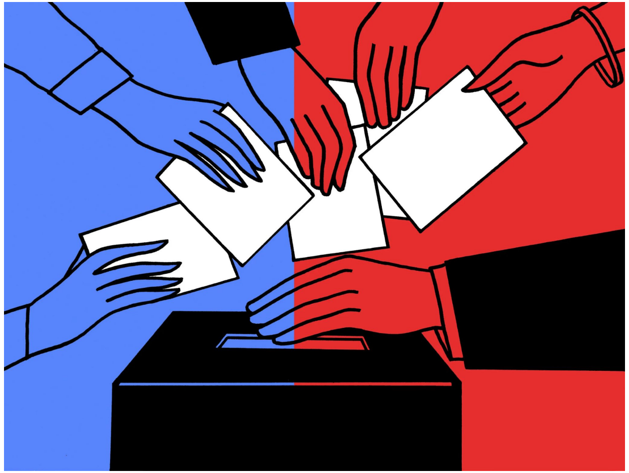
2 Consensus: Proof of Work and BFT

PROOF OF WORK

PoW



Source: Arthur D. Little



BFT

Aspect	Proof of Work (PoW)	Byzantine Fault Tolerance (BFT)
Consensus Method	Competition-based mining	Voting-based agreement
Block Production	Through solving cryptographic puzzles	Through leader proposal and voting
Node Identity	Anonymous, anyone can join	Known participants
Communication	Minimal between nodes	Heavy message exchange
Fault Tolerance	~51% honest computing power needed	Typically handles up to 33% Byzantine nodes
Performance	Lower throughput, higher latency	Higher throughput, lower latency
Security	Hard to attack	Mathematical proof of safety
Network Load	Lower network overhead	Higher network overhead
Incentives	Block rewards and fees	Usually no direct incentives