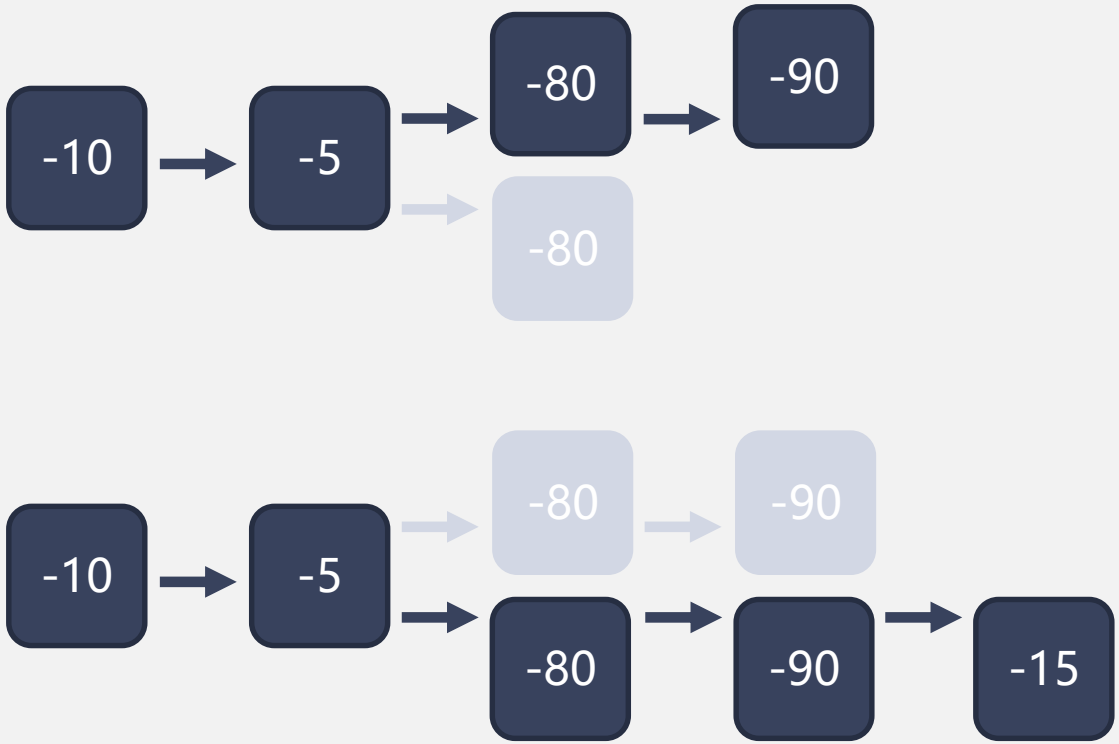
How to prevent double spending for Libra

黃郁傑 林宸熏 楊政道

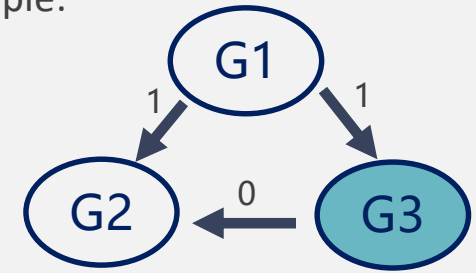
Double Spending

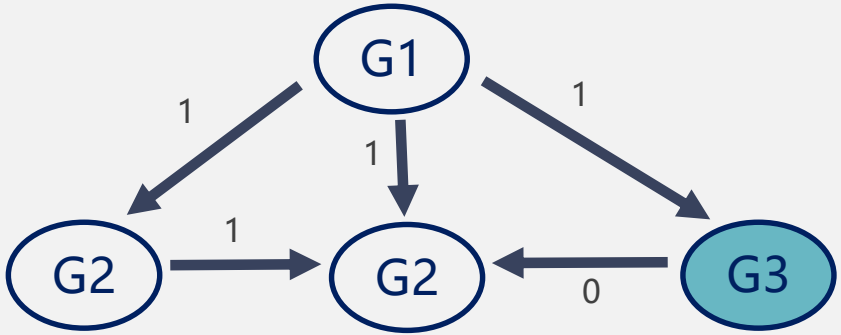


BFT protocol

Byzantine failure

- Traitor nodes send conflicting messages
  - Which leads to an incorrect result
- Cause:
  - Flaky nodes
  - Malicious nodes
- Example:



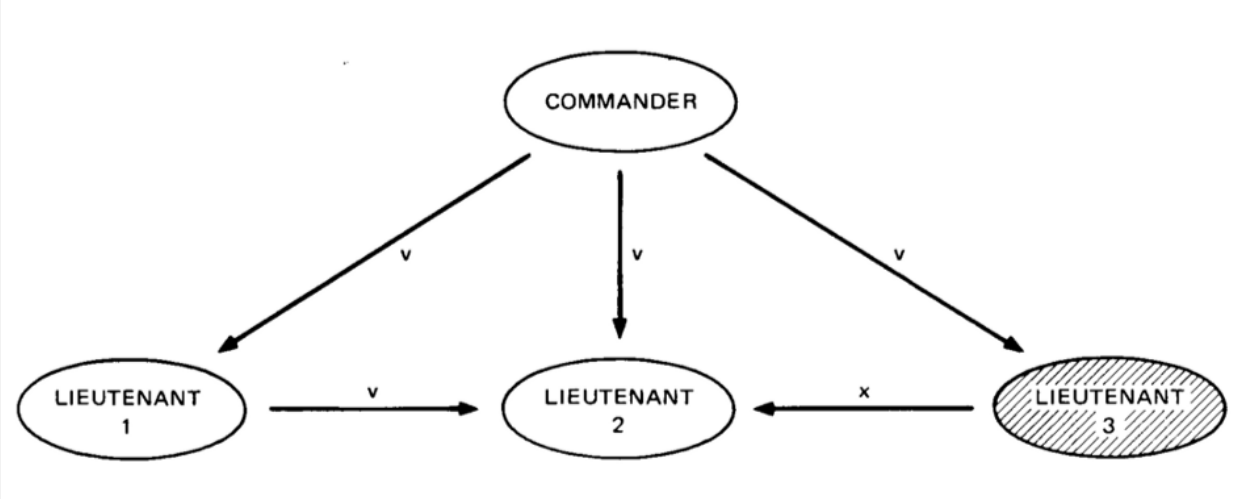


The question

If we want all the generals to get the “same” value…

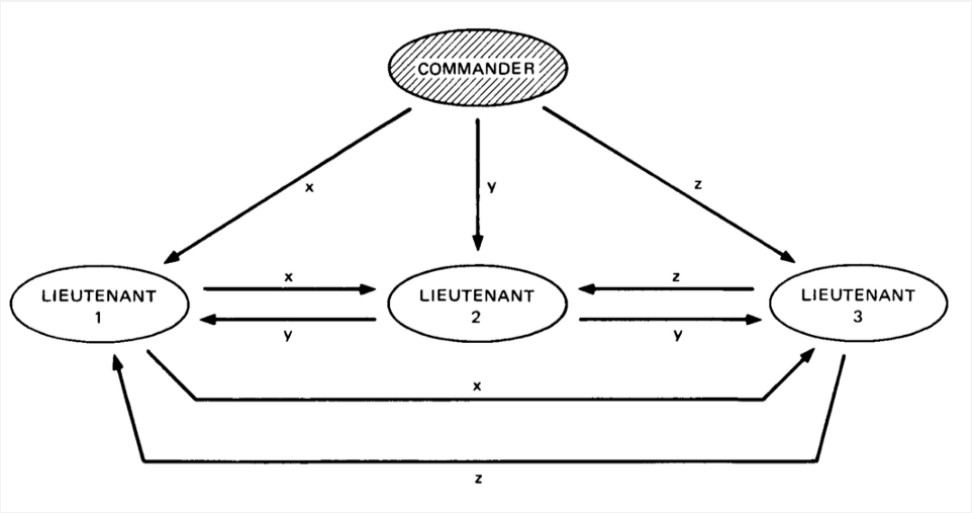
How many traitors can we be tolerated?

Situation 1 (when commander is not a traitor)



- L2 <- max(*v*,*v*,*x*) == *v*
- L2 can get the “correct” value from commander

Situation 2 (when commander is a traitor)



- L1 <- max(x,y,z) | L2 <- max(x,y,z) | L3 <- max(x,y,z)
- L2 can get the “same” value from commander

Result

Lemma: **No** solution for **3m+1** generals with **>m** traitors.

Proof:

1. Assume solution exists.

2. Use solutions to solve **1** traitors **3** generals case.

We know 2 is impossible.

Hence solution must not exist.

Byzantine Fault Tolerance (BFT)

How might you build such a system ??

The Lamport, Pease and Shostak Algorithm

The Lamport, Pease and Shostak Algorithm

Algorithm OM(0)

1. The general sends his value to every lieutenant.
2. Each lieutenant uses the value he receives from the general.

Algorithm OM(m), m > 0

1. The general sends his value to each lieutenant.
2. For each i, let v_i be the value lieutenant i receives from the general. Lieutenant i acts as the general in Algorithm OM(m-1) to send the value v_i to each of the n-2 other lieutenants.
3. For each i, and each $j \neq i$, let v_i be the value lieutenant i received from lieutenant j in step 2 (using Algorithm (m-1)). Lieutenant i uses the value majority (v_1, v_2, ... v_n).<>

Lamport's Algorithm Definition

Running time (time complexity)

m	Time complexity
0	O(n)
1	O(n^2)
2	O(n^3)
3	O(n^4)

Practical Byzantine Fault Tolerance (PBFT)

FEATURE OF PRACTICAL BYZANTINE FAULT TOLERANCE

- Total nodes > 3 X faulty nodes
- Every node know each other
- Each action has a sequence number
- Only one leader node
- Nodes can ask to change leader (view-change)

WHY N MUST BIGGER THAN 3F

N： total nodes

F ： faulty nodes (may be faulty or not responding)

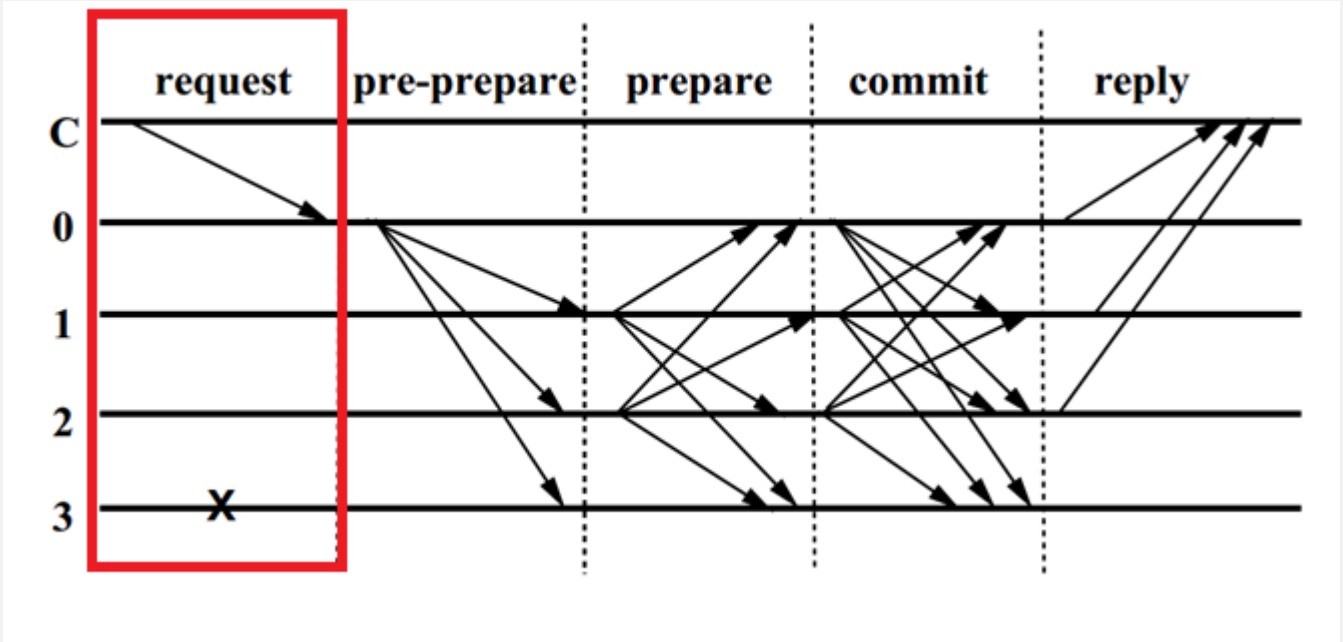
01 **Threshold = N-F** Must make the decision within N-F nodes

02 **(N-F)-F>F** To ensure normal nodes more than faulty nodes

OPERATION OF PRACTICAL BYZANTINE FAULT TOLERANCE

1.Request

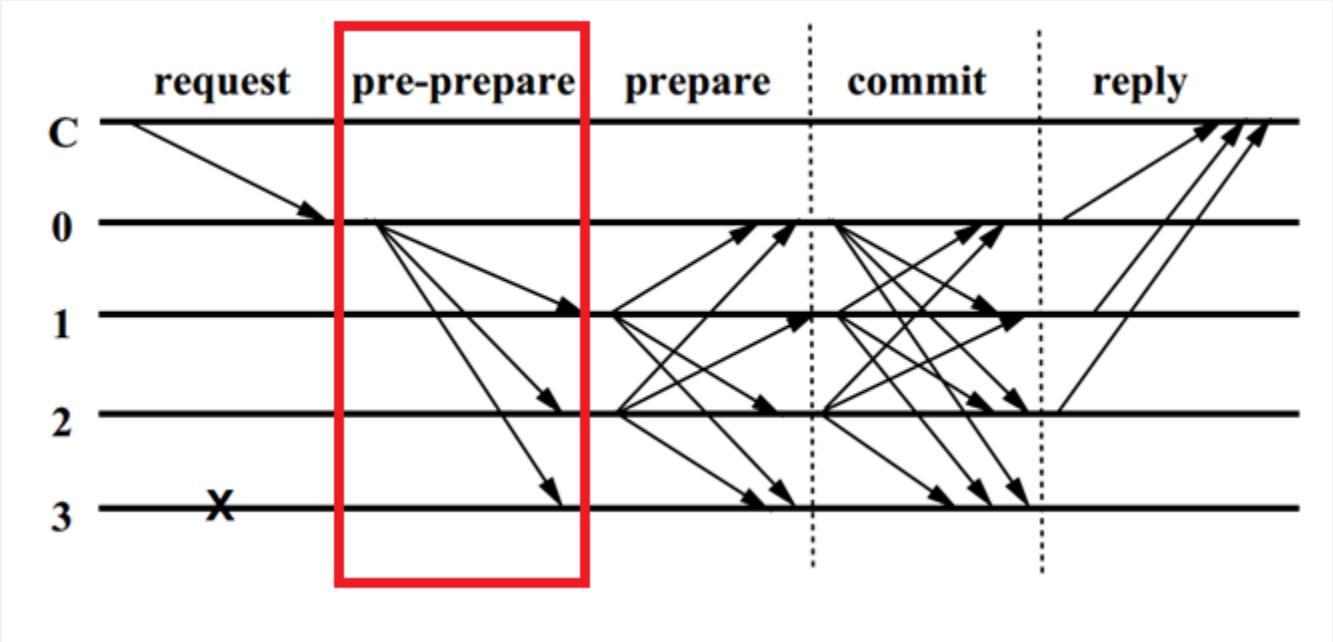
LEADER



OPERATION OF PRACTICAL BYZANTINE FAULT TOLERANCE

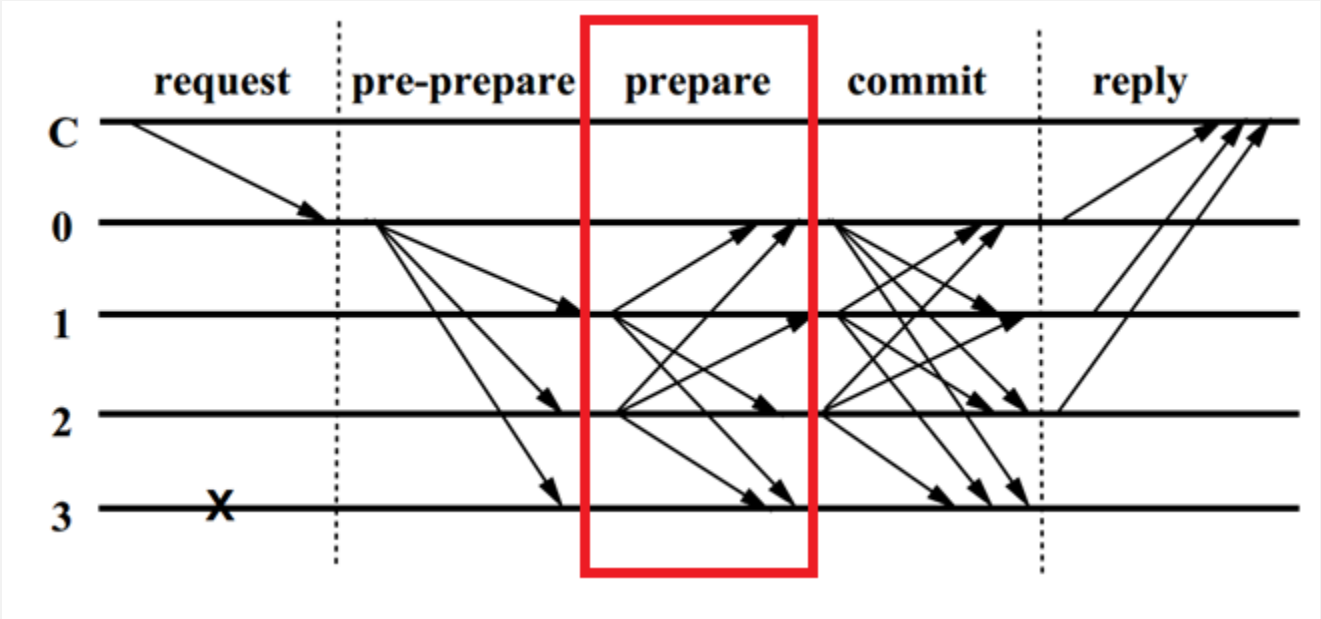
2.Pre-prepare

LEADER



OPERATION OF PRACTICAL BYZANTINE FAULT TOLERANCE

3.Prepare： decide whether the request is legal
one node can make decision if it get more than 2F+1 votes

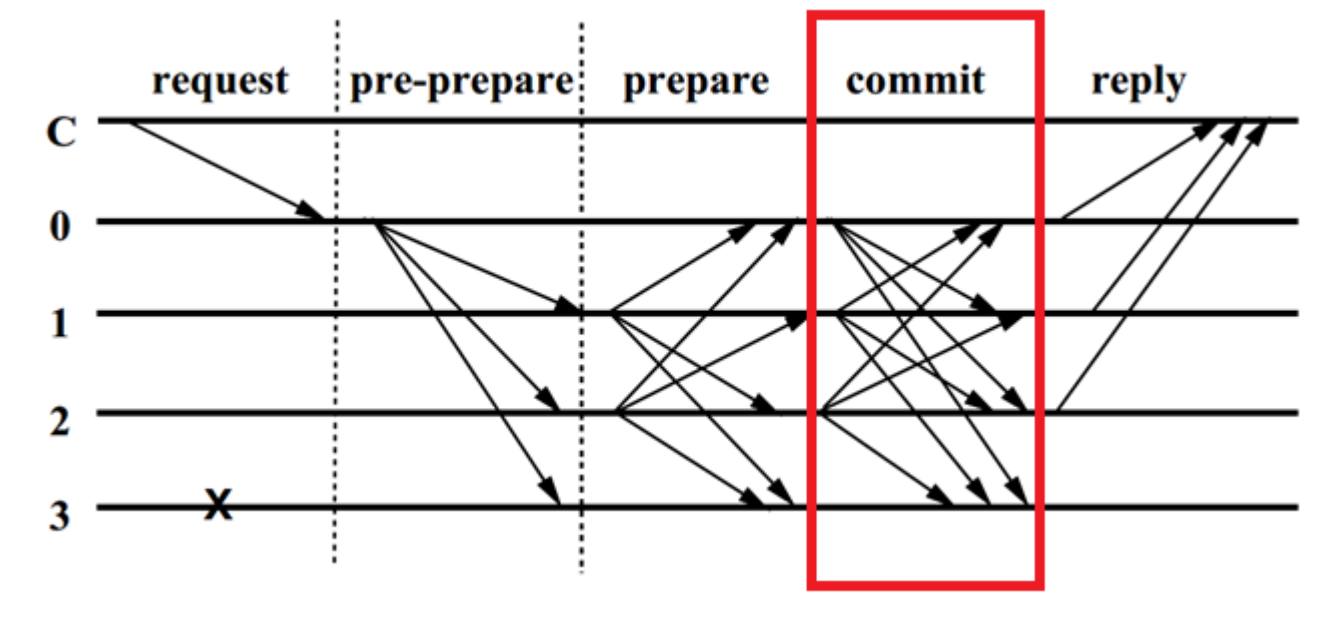


OPERATION OF PRACTICAL BYZANTINE FAULT TOLERANCE

4.Commit：vote

one node can make decision if it get more than 2F+1 votes

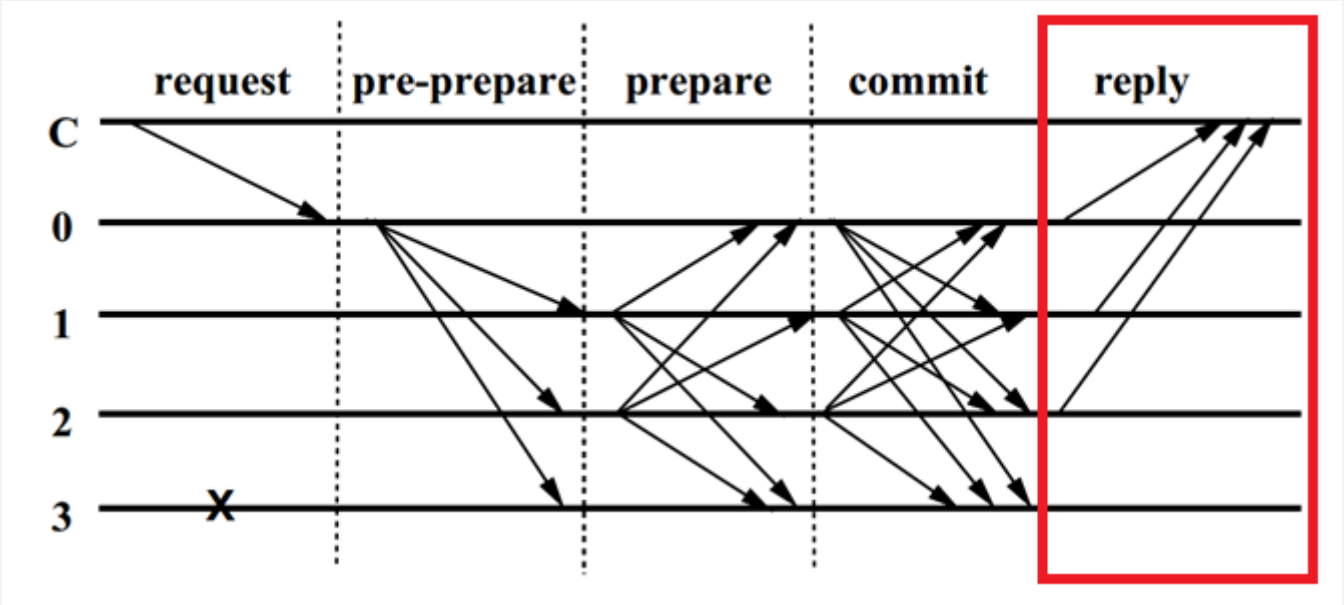
LEADER



OPERATION OF PRACTICAL BYZANTINE FAULT TOLERANCE

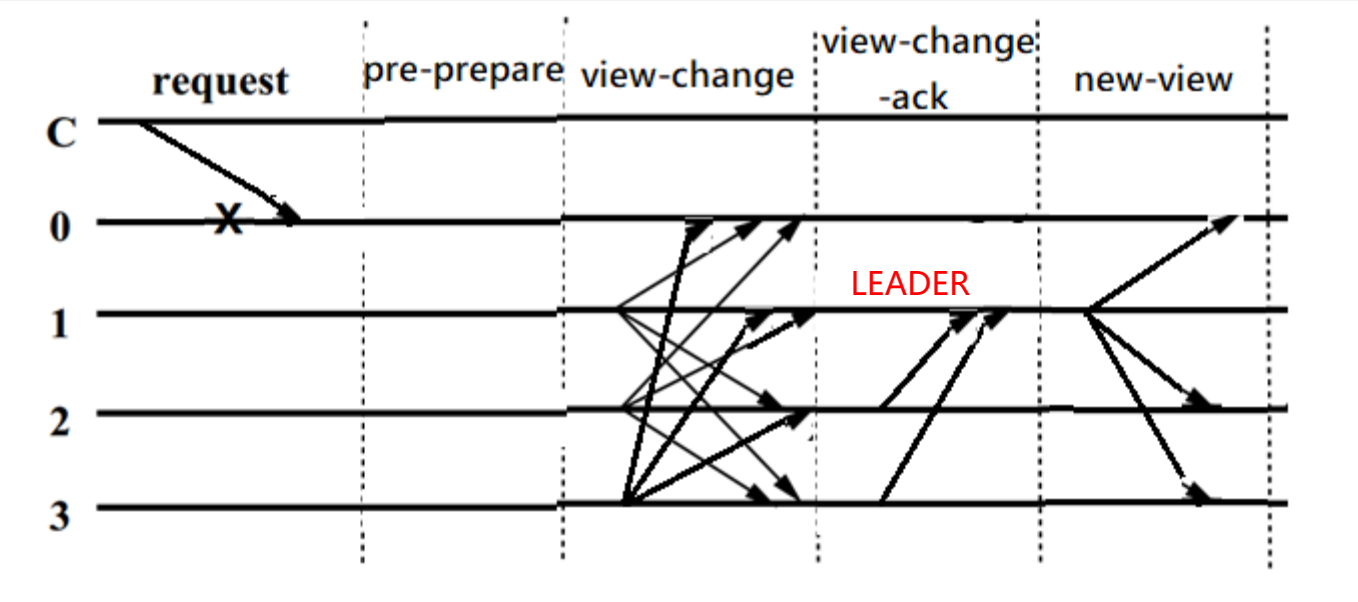
5.Reply：make final decision if it get more than F+1 votes

LEADER



When 0 is a bad leader

LEADER



ADVANTAGES OF PRACTICAL BYZANTINE FAULT TOLERANCE

01 **Contain fault tolerance**

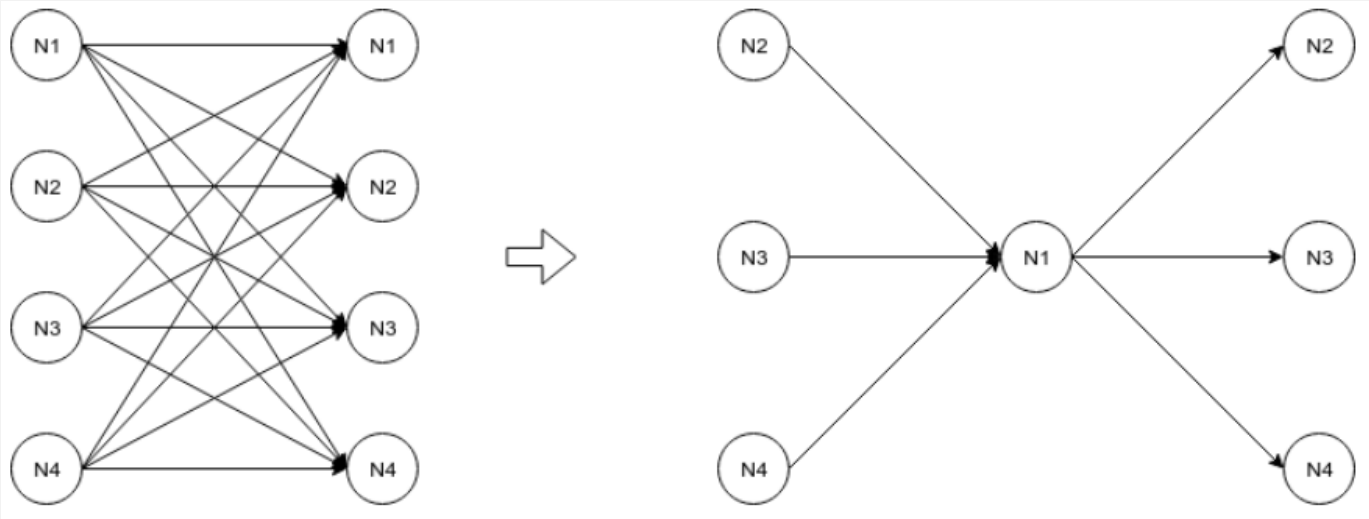
02 **No need to launch token**

DISADVANTAGES OF PRACTICAL BYZANTINE FAULT TOLERANCE

01 **Leader based**

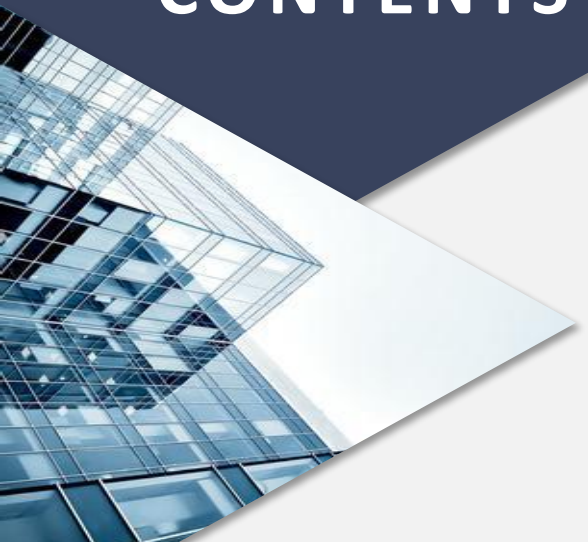
02 **Closure property**

03 **High complexity**



O(N^2) O(N)

CONTENTS



Round

user

transaction

leader

block

nodes

N – f vote

f+1 timeout

Partial synchrony

Internet delay

DoS

Communication delay

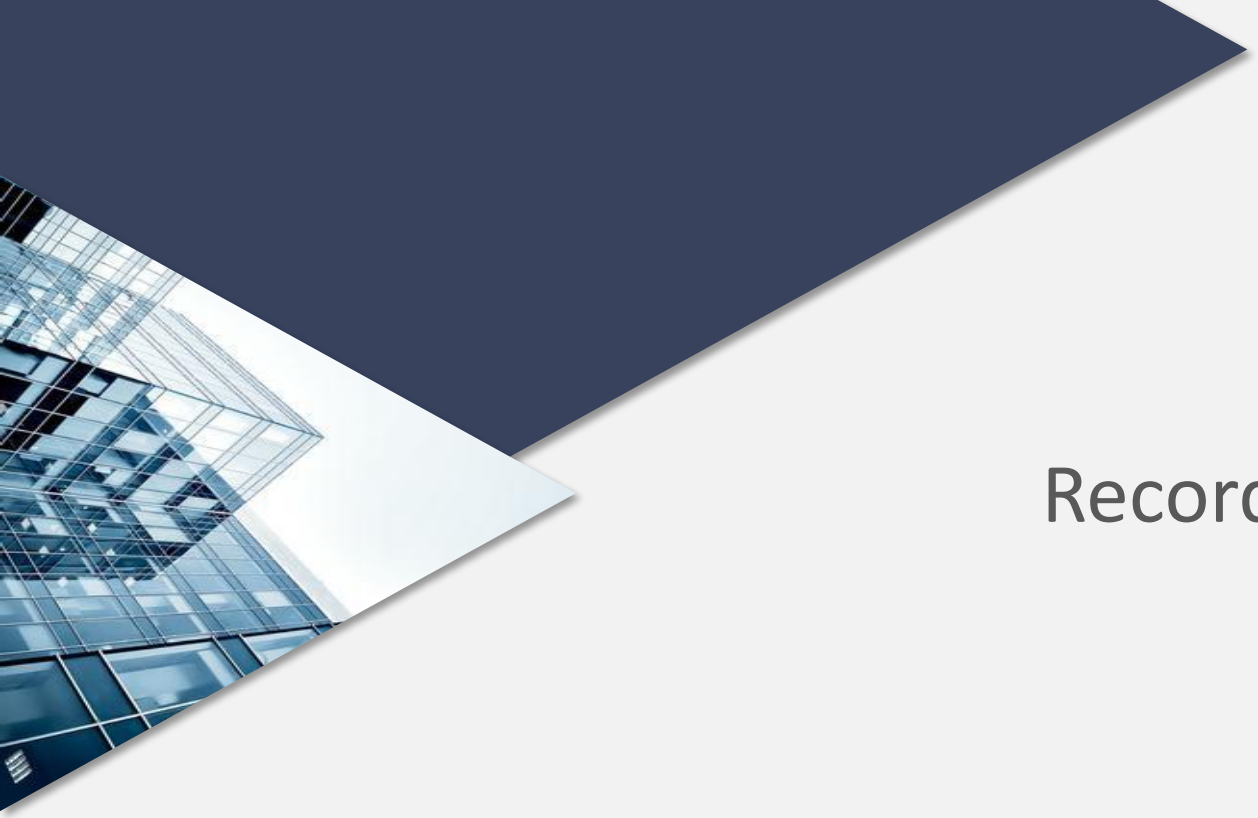
Syn riod

Delay

Asynchrony：waiting for infinite time

BFT：waiting for at most Δ

LBFT：waiting for Δ +max(t,GST)



Record

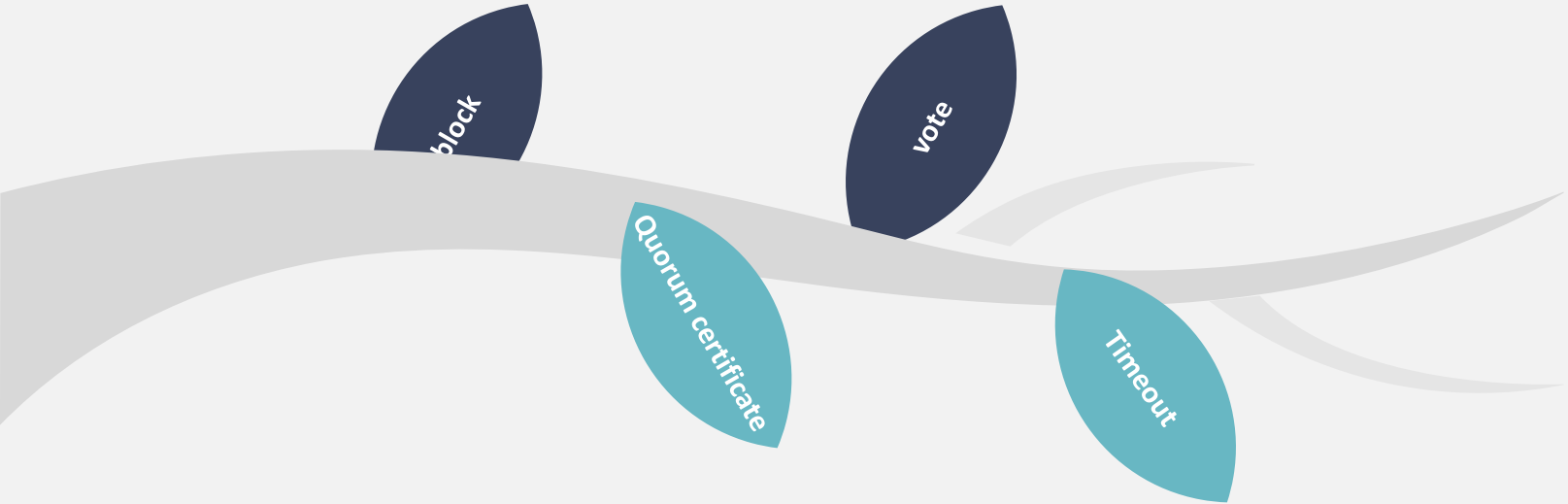
Records

Block

由leader在指定的round提案

vote

Node投票同意block和執行後的state



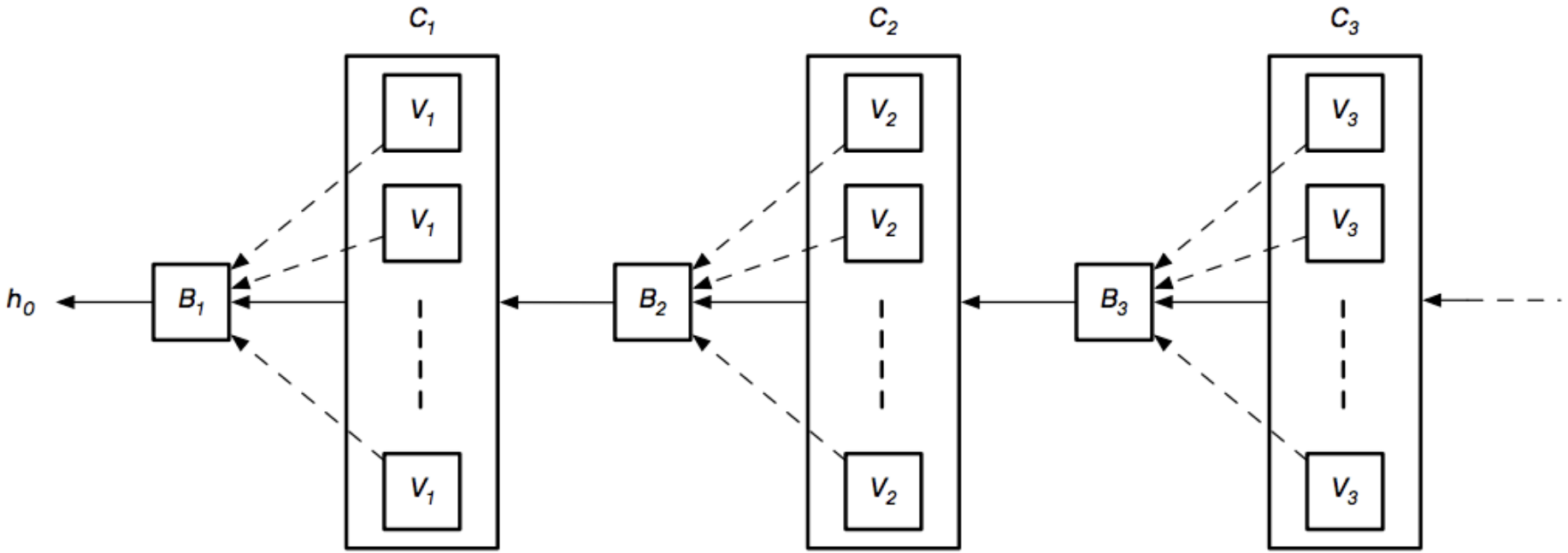
Quorum certificate

Vote的集合並帶有選擇性欄位commitment

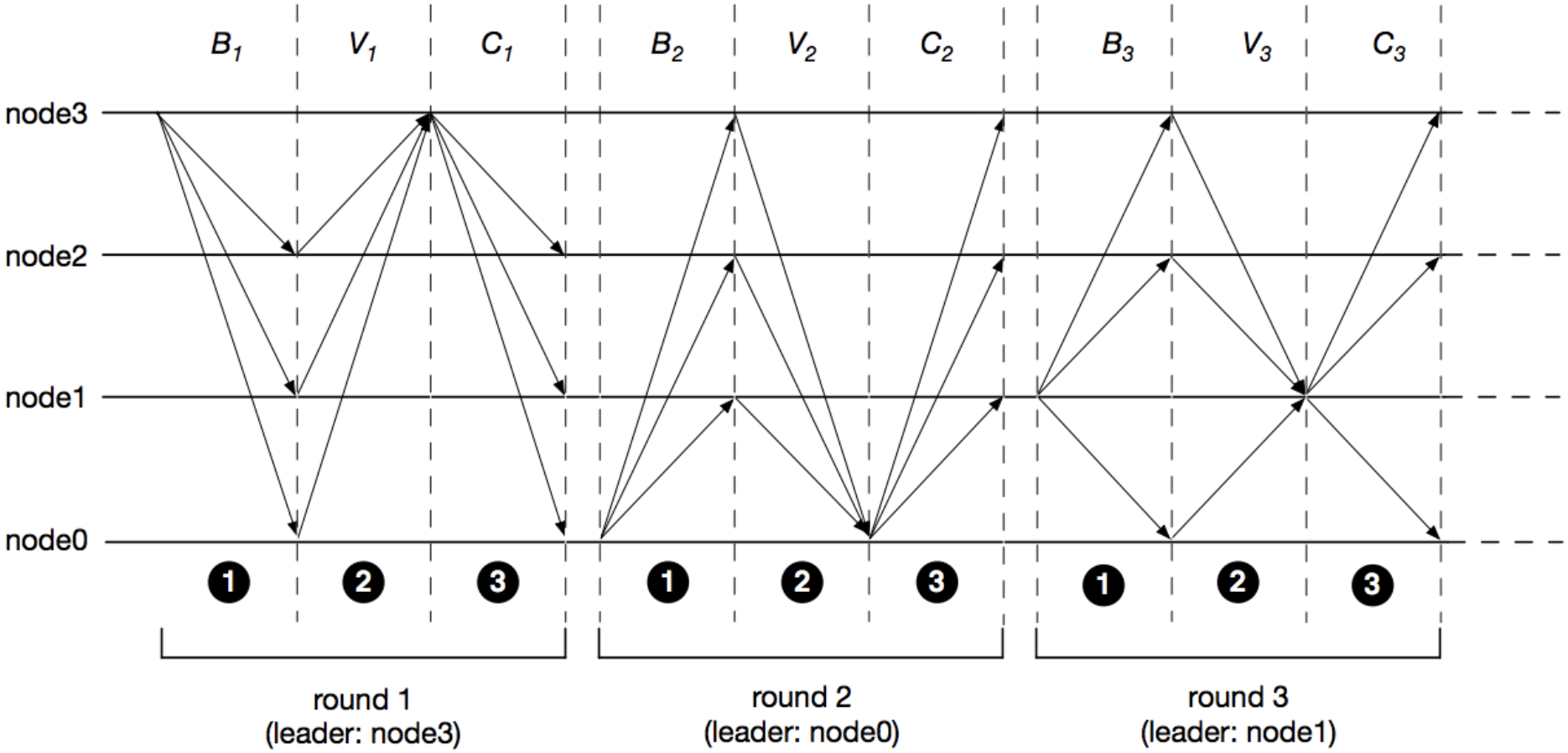
Timeout

投票表示更換leader

每個部分都有author和signature

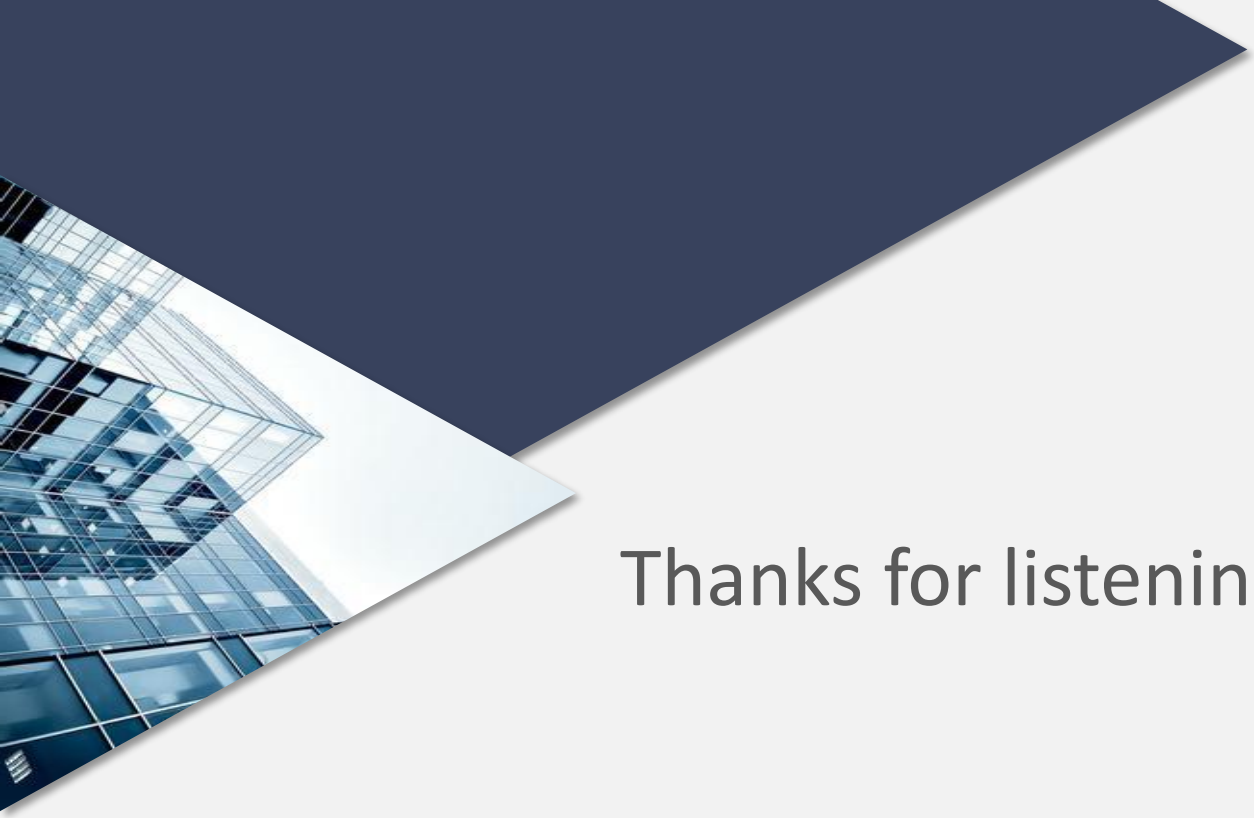

C_1
C_2
C_3
V_1
V_1
V_1
V_2
V_2
V_2
V_3
V_3
V_3
h_0
B_1
B_2
B_3

Protocol


B_1
V_1
C_1
B_2
V_2
C_2
B_3
V_3
C_3
node3
node2
node1
node0
1
2
3
1
2
3
1
2
3
round 1
(leader: node3)
round 2
(leader: node0)
round 3
(leader: node1)

聖人大盜 電影心得

這部聖人大盜的電影中，多次提到區塊鍊應用，主角團們希望透過區塊鍊的技術結合金融革新，來達到他們創業的目標，同時也是一種追逐夢想的故事。然而看似"去中心化"的中心理念，卻在後續跟政府的合作報告中無法實現，也因為有這些弊端，主角團們才開始思考在夢想與現實妥協是不是一個正確的決定。最後，主角團為了不讓這些社會上游的人持續把持住這個社會，決定最初反撲。我覺得，整片故事中，傳遞了很強的金融體系不公正的問題，因此，在這樣的時空背景之下，區塊練變成一種改正社會風氣的正義，也透過主角團們實現區塊鍊的應用來傳遞社會正義的實現。



Thanks for listening!