Zyzzyva: Speculative Byzantine Fault Tolerance

Mengxiao Lin, Jiayu Liu

What is Zyzzyva

How does it work

Why choose Zyzzyva

Zyzzyva, a protocol that uses speculation to reduce the cost and simplify the design of Byzantine fault tolerant state machine replication.

How does Zyzzyva work

Sub-protocols

Agreement

View change

Checkpoint

Agreement

The agreement protocol orders requests for execution by the replicas.

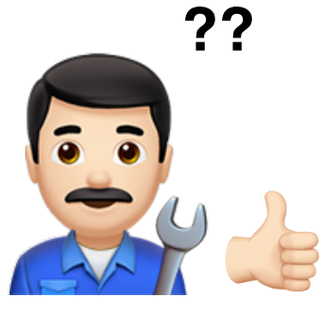
Timestamp

$$m = \langle \text{REQUEST}, o, t, c \rangle \sigma_c$$

Operation Client ID

$$OR = \langle\langle \text{ORDER-REQ}, v, n, h_n, d, ND\rangle\sigma_p\ , m\rangle$$

History Viewstamp Sequence number Number of requests $h_n = H(h_{n-1}, d)$



$$OR = \langle\langle \text{ORDER-REQ}, v, n, h_n, d, ND\rangle\sigma_p\ , m\rangle$$

$$d == H(m)$$

$$n == max_n + 1$$

$$h_n == H(h_{n-1}, d)$$

Reply

$\langle\langle \text{SPEC-RESPONSE}, v, n, h_n, H(r), c, t\rangle\sigma_i\ , i, r, OR\rangle$

???

$3f + 1$

R_i **R_j**


$$\langle\langle \text{SPEC-RESPONSE}, v, n, h_n, H(r), c, t\rangle\sigma_i \ , i, r, OR\rangle$$

$$\langle\langle \text{SPEC-RESPONSE}, v, n, h_n, H(r), c, t\rangle\sigma_j \ , j, r, OR\rangle$$

It's a MATCH!

$$3f + 1$$

???

$$[\ 2f + 1, 3f\ ]$$

$$m = \langle \text{REQUEST}, o, t, c \rangle \sigma_c$$

$\langle \text{COMMIT}, c, CC \rangle \sigma_c$

Commit Certificate

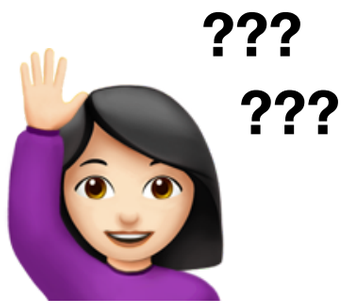
A list of 2f+1 replicas & their signed portion of SPEC-RESPONSE

$\langle \text{SPEC-RESPONSE}, v, n, h_n, H(r), c, t \rangle \sigma_i$

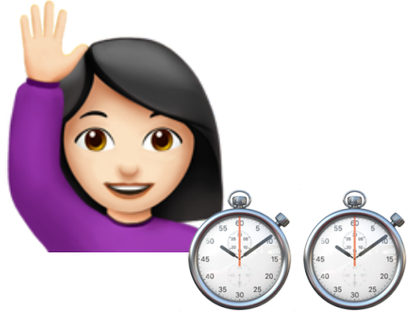



$\langle \text{LOCAL-COMMIT}, v, d, h, i, c \rangle \sigma_i$



$$[\,0, 2f + 1\,)$$



$$m = \langle \text{REQUEST}, o, t, c \rangle \sigma_c$$

Cached response Cached response Cached response

New OR

Cached OR

$$\langle \text{CONFIRM-REQ}, v, m, i \rangle \sigma_i$$

$\mathbf{R_i}$ $\mathbf{R_j}$


$$\langle\langle \text{SPEC-RESPONSE}, v, n, h_n, H(r), c, t\rangle\sigma_i \ , i, r, \text{OR}\rangle$$

$$\langle\langle \text{SPEC-RESPONSE}, v, n, h_n, H(r), c, t\rangle\sigma_j \ , j, r, \text{OR}\rangle$$

It's a MATCH!

$$\text{OR} = \langle\langle \text{ORDER-REQ}, v, n, h_n, d, \text{ND}\rangle\sigma_p \ , m\rangle$$

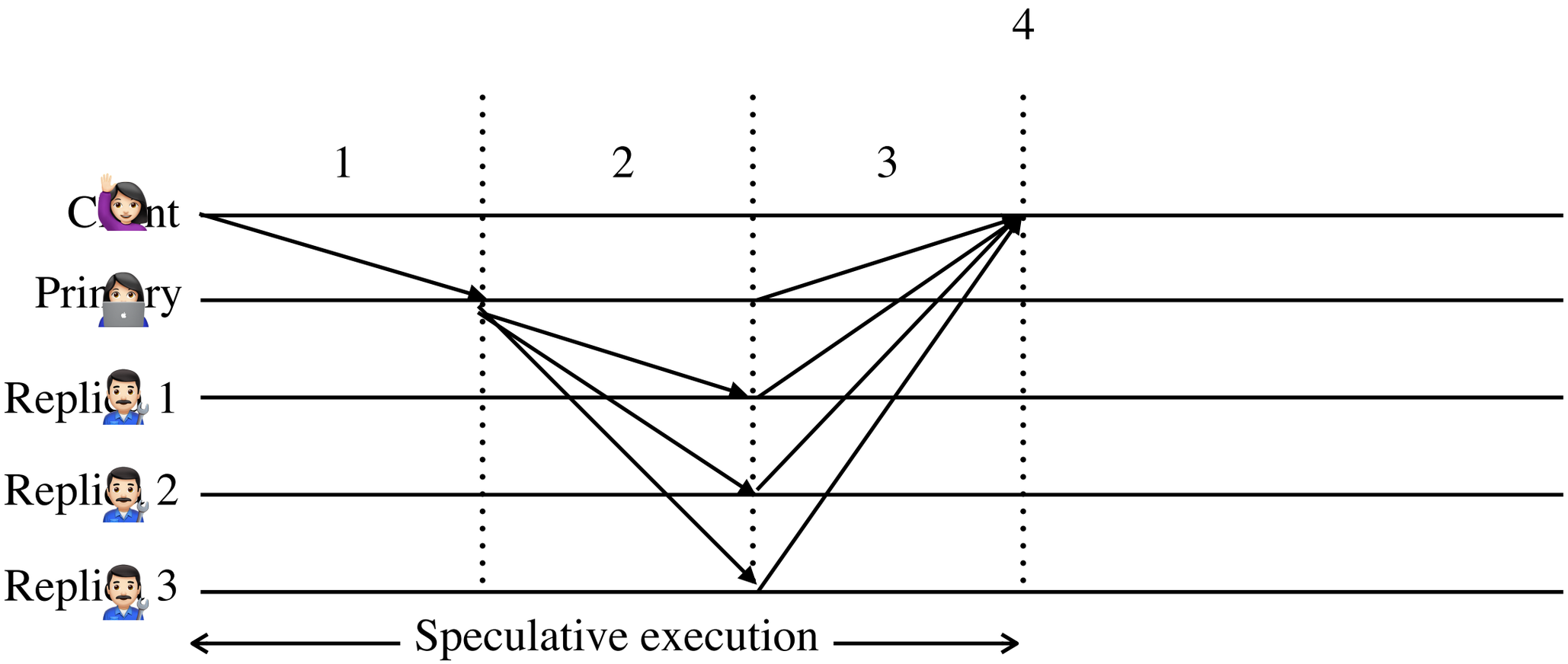
$\langle \mathrm{POM}, \mathrm{v}, \mathit{POM} \rangle \sigma_c$

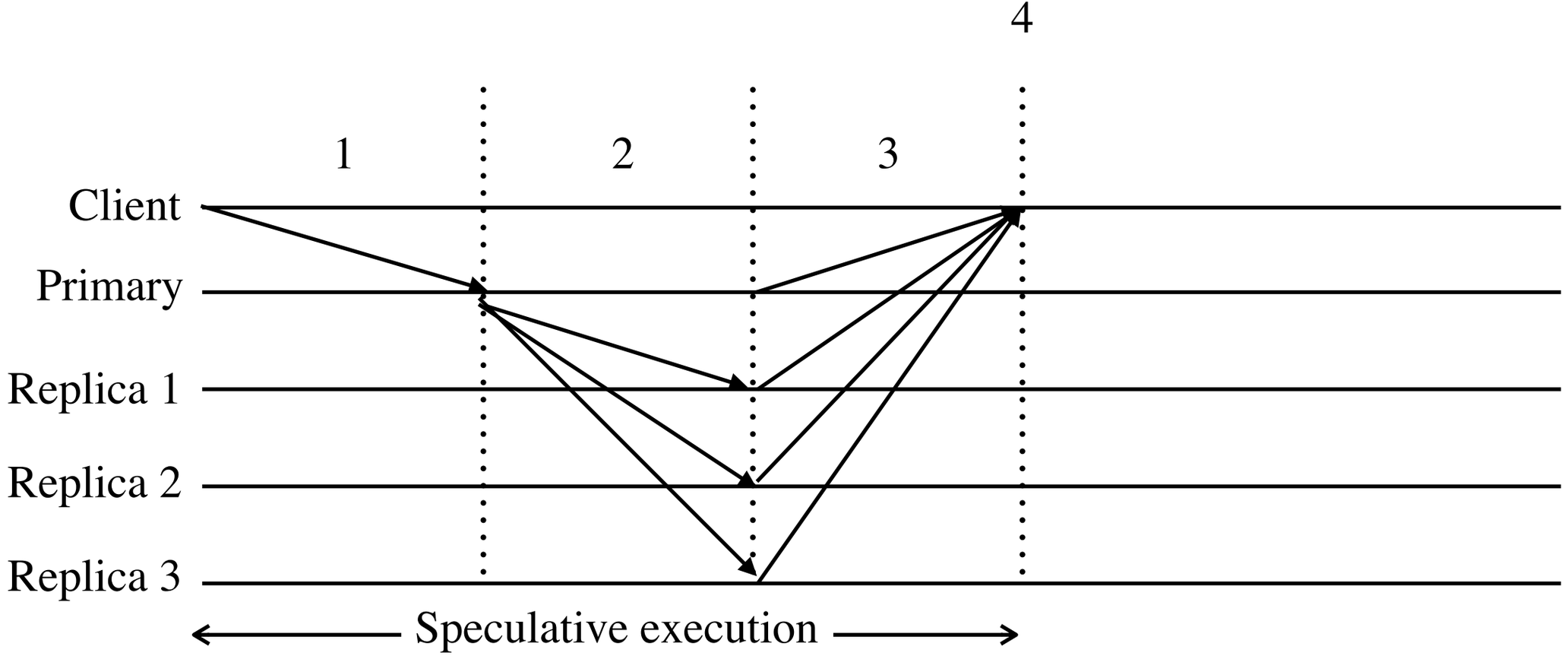
View change

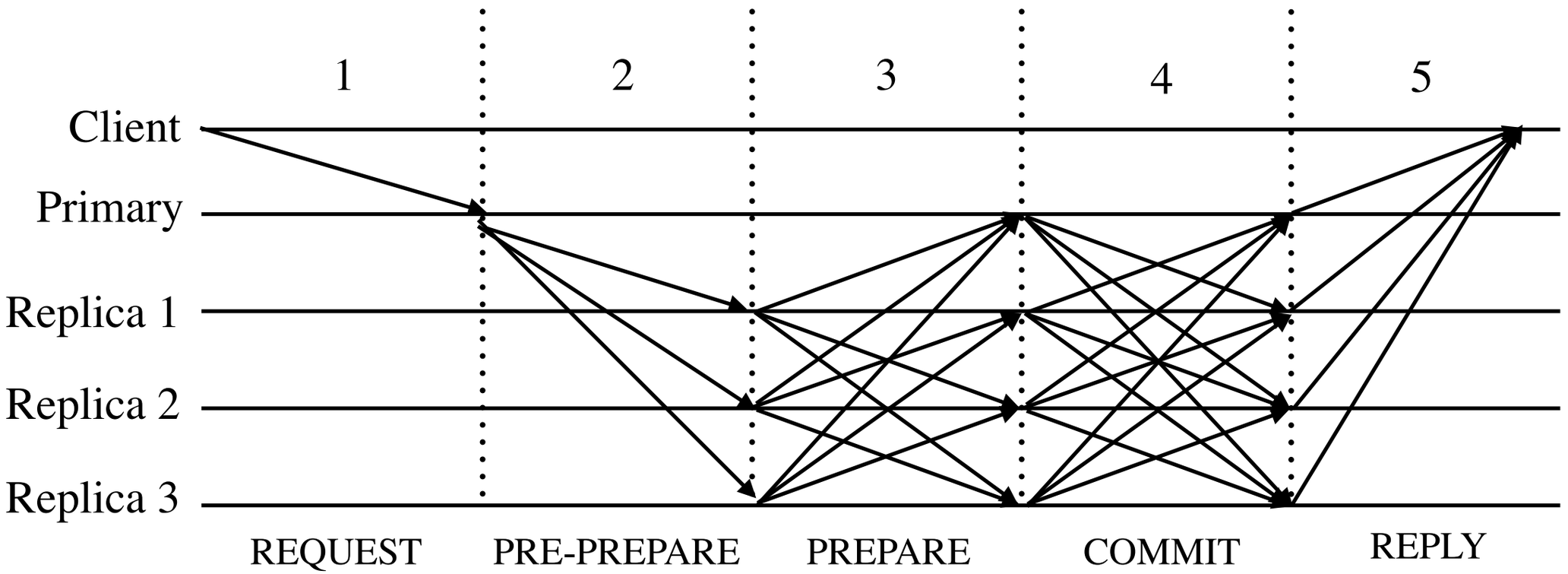
View change

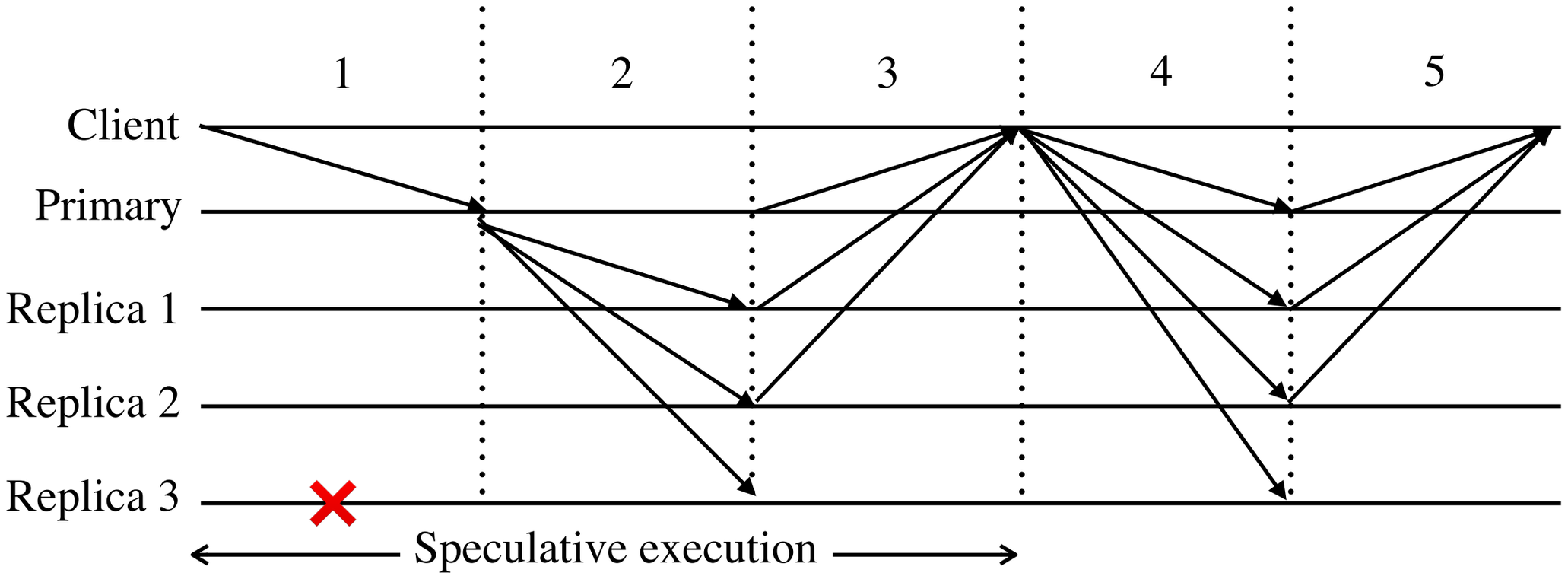
View change

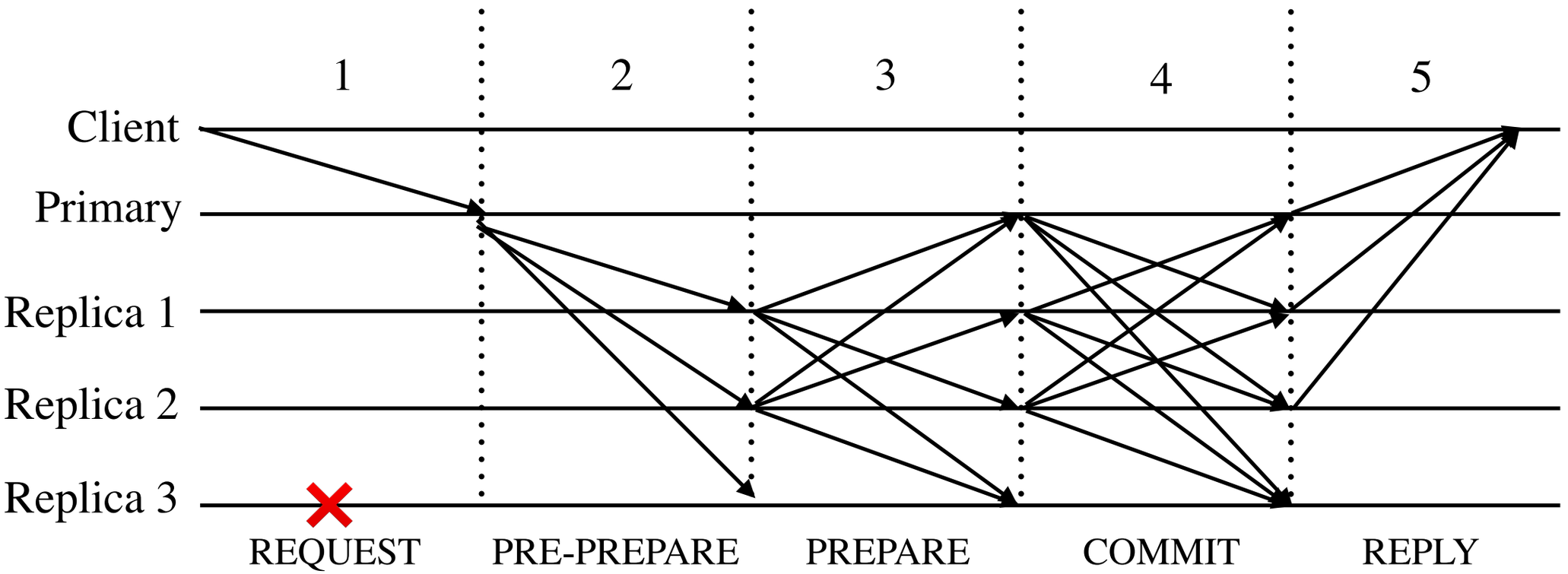
View change


4
1
2
3
Client
Primary
Replica 1
Replica 2
Replica 3
Speculative execution


1
2
3
4
Client
Primary
Replica 1
Replica 2
Replica 3
Speculative execution

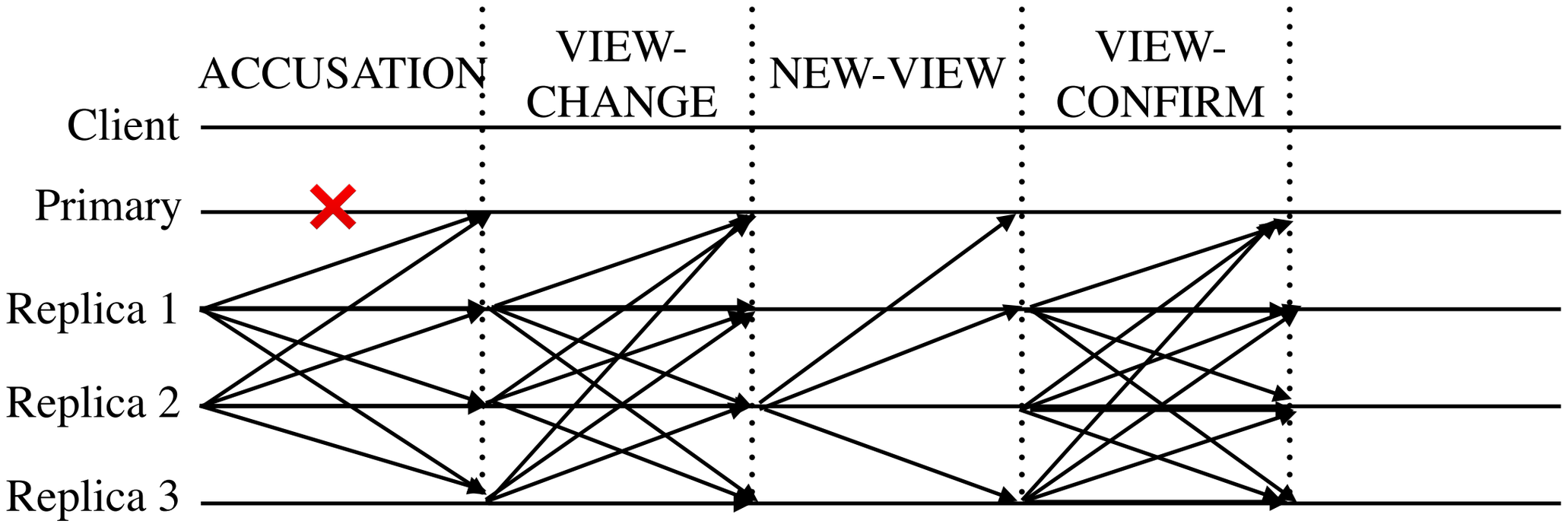

1
2
3
4
5
Client
Primary
Replica 1
Replica 2
Replica 3
REQUEST
PRE-PREPARE
PREPARE
COMMIT
REPLY


1
2
3
4
5
Client
Primary
Replica 1
Replica 2
Replica 3
Speculative execution

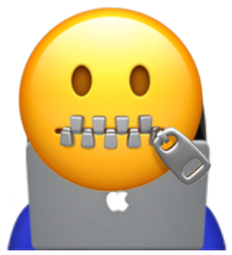

1
2
3
4
5
Client
Primary
Replica 1
Replica 2
Replica 3
REQUEST
PRE-PREPARE
PREPARE
COMMIT
REPLY

View change

View Change Protocol when f = 1

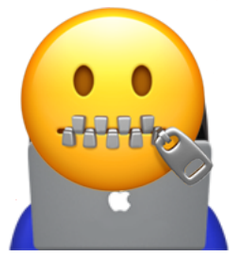


⟨ACCUSATION⟩σ_2

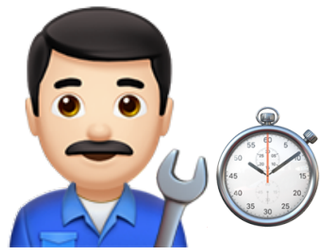


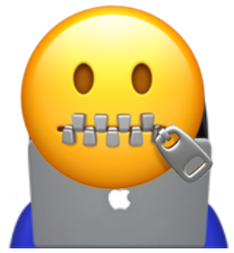
$\langle$NEW-VIEW, v+1, P$\rangle\sigma_2$

P = 2f+1 <VIEW-CHANGE> messages



⟪VIEW-CHANGE, v+2⟫σ_2





$\langle$VIEW-CHANGE, v+2$\rangle\sigma_1$

$[\ 2f + 1, 3f\ ]$

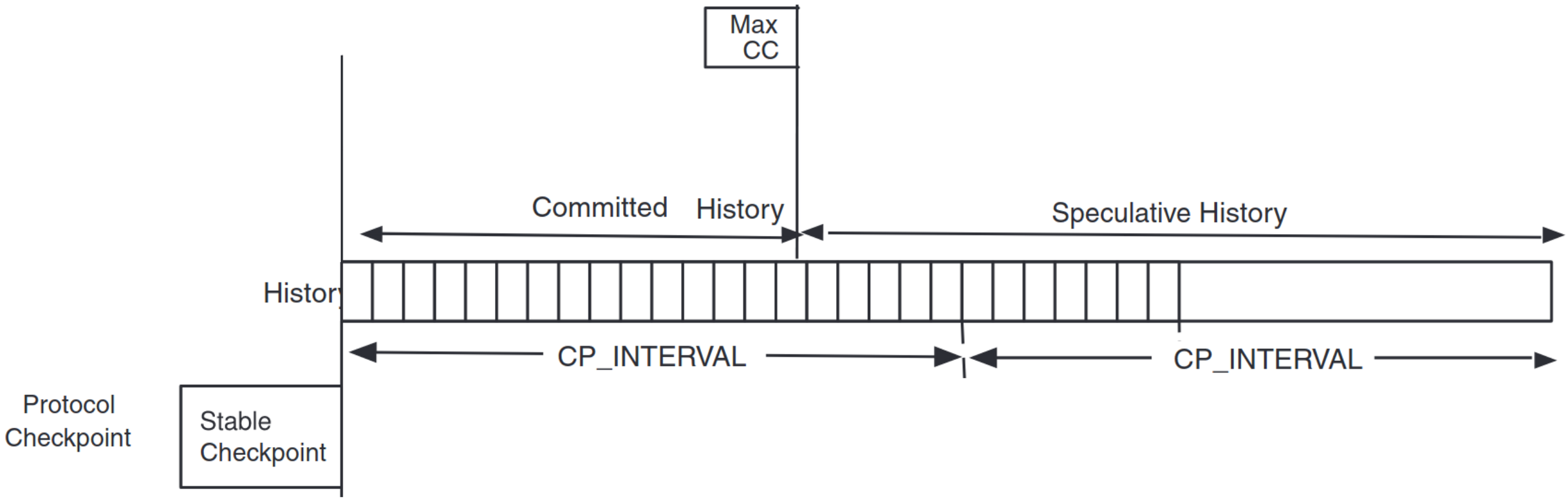
<VIEW-CHANGE, CC, v+1>

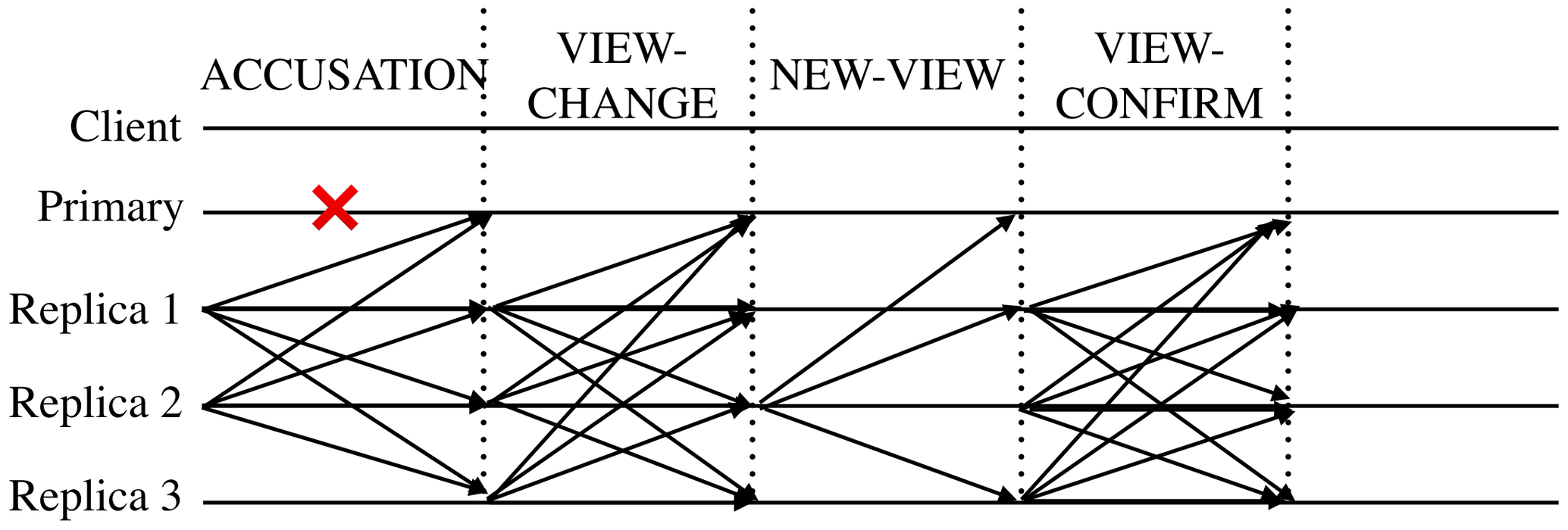
???

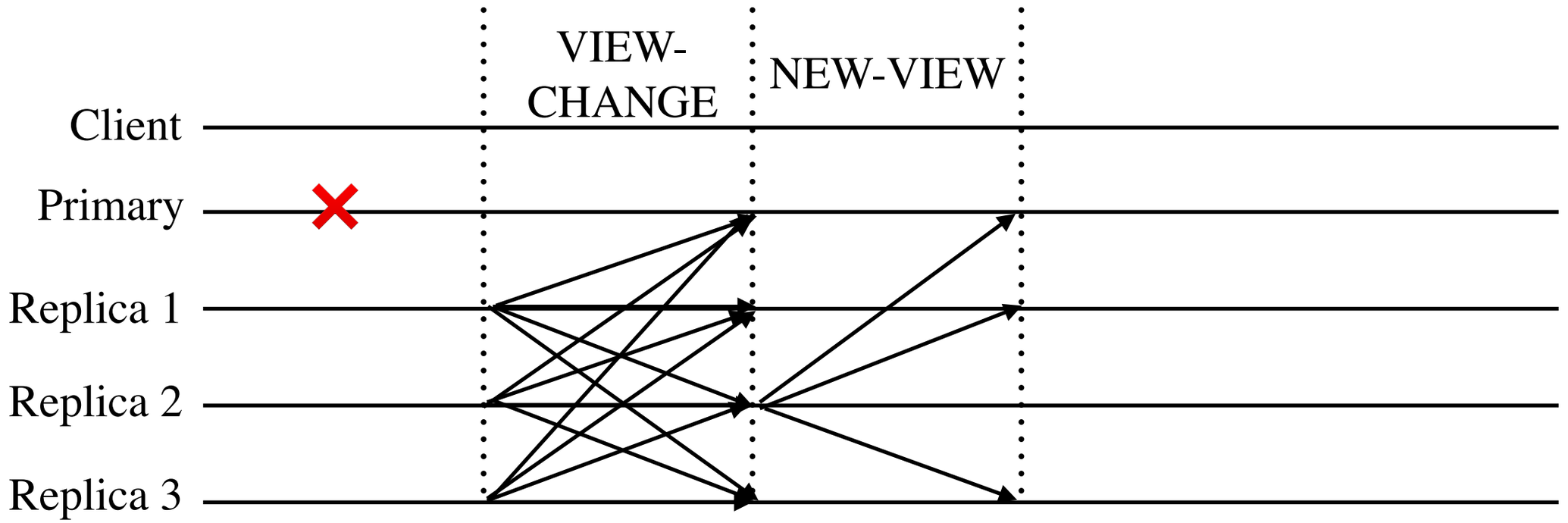
3f+1

<VIEW-CHANGE, CC, O, v+1>

Checkpoint


Max
CC
Committed
History
Speculative History
History
CP_INTERVAL
CP_INTERVAL
Protocol
Checkpoint
Stable
Checkpoint


ACCUSATION
VIEW-
CHANGE
NEW-VIEW
VIEW-
CONFIRM
Client
Primary
Replica 1
Replica 2
Replica 3


VIEW-
CHANGE
NEW-VIEW
Client
Primary
Replica 1
Replica 2
Replica 3

Zyzzyva, a protocol that uses speculation to reduce the cost and simplify the design of Byzantine fault tolerant state machine replication.

Thank you