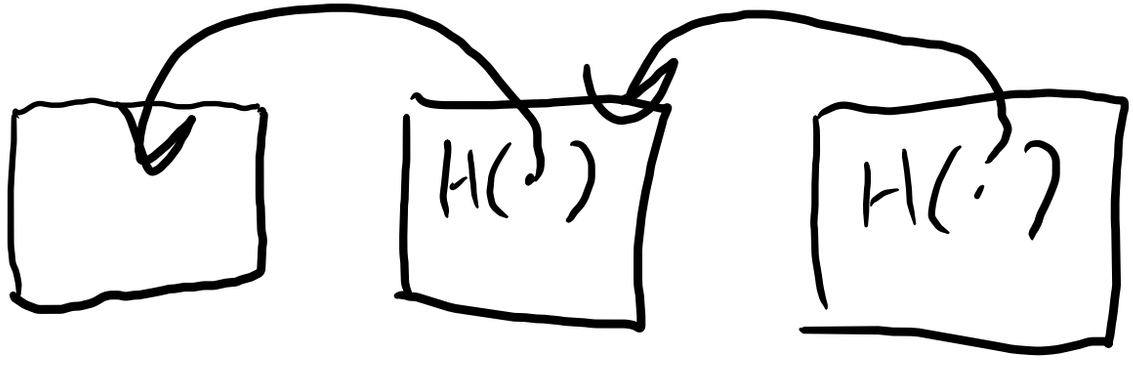
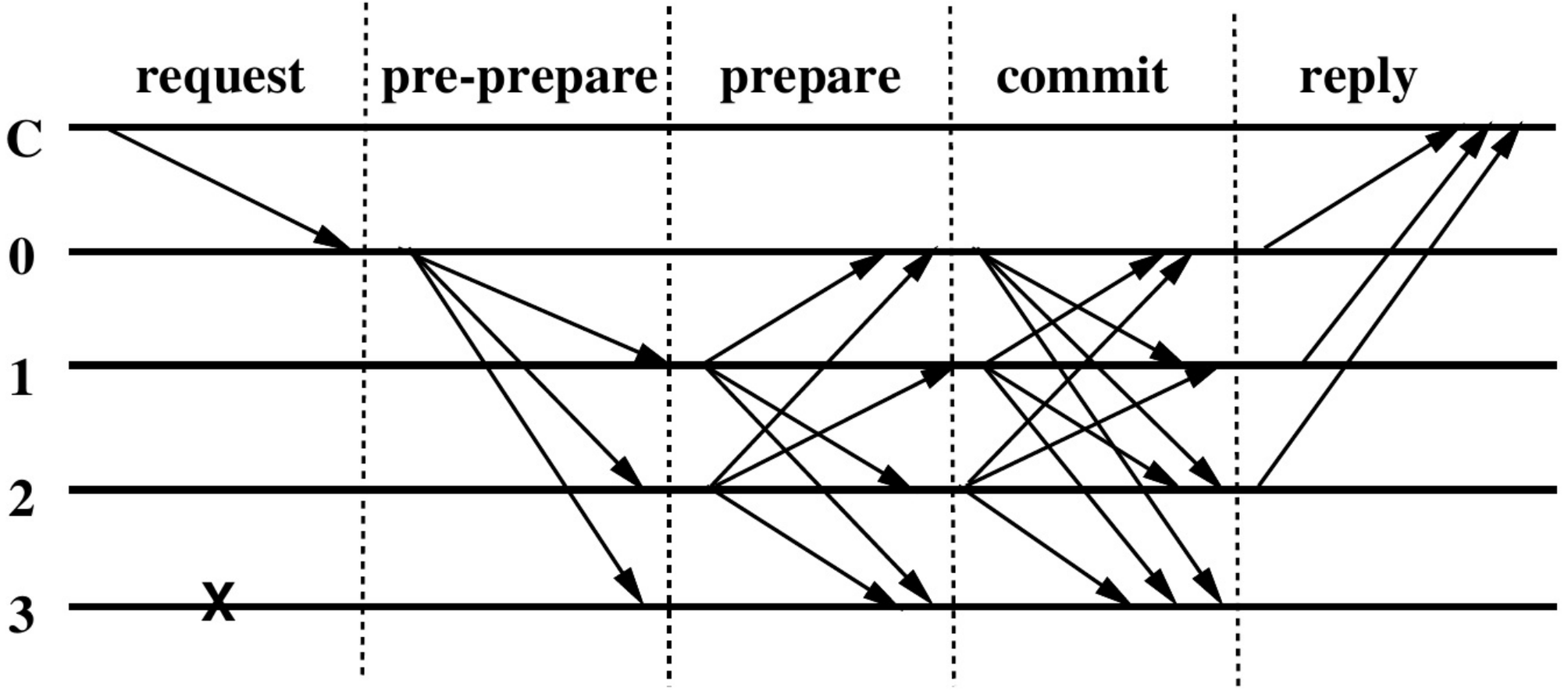
GST △

⟨amount, recipient, memo⟩

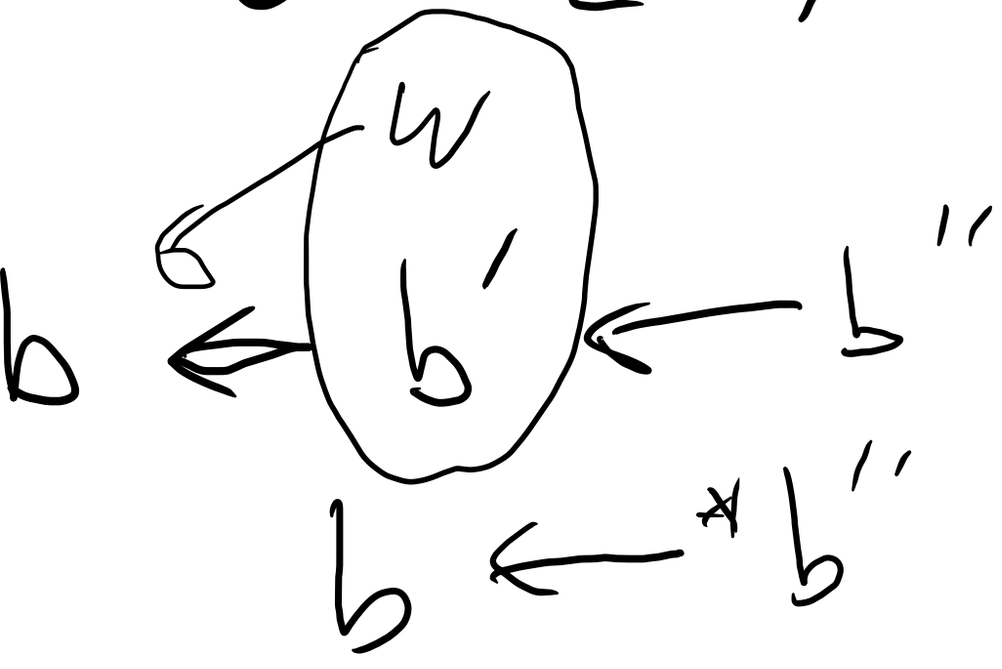
1. Coin Distribution | Proof-of-work
2. Double-spend problem |



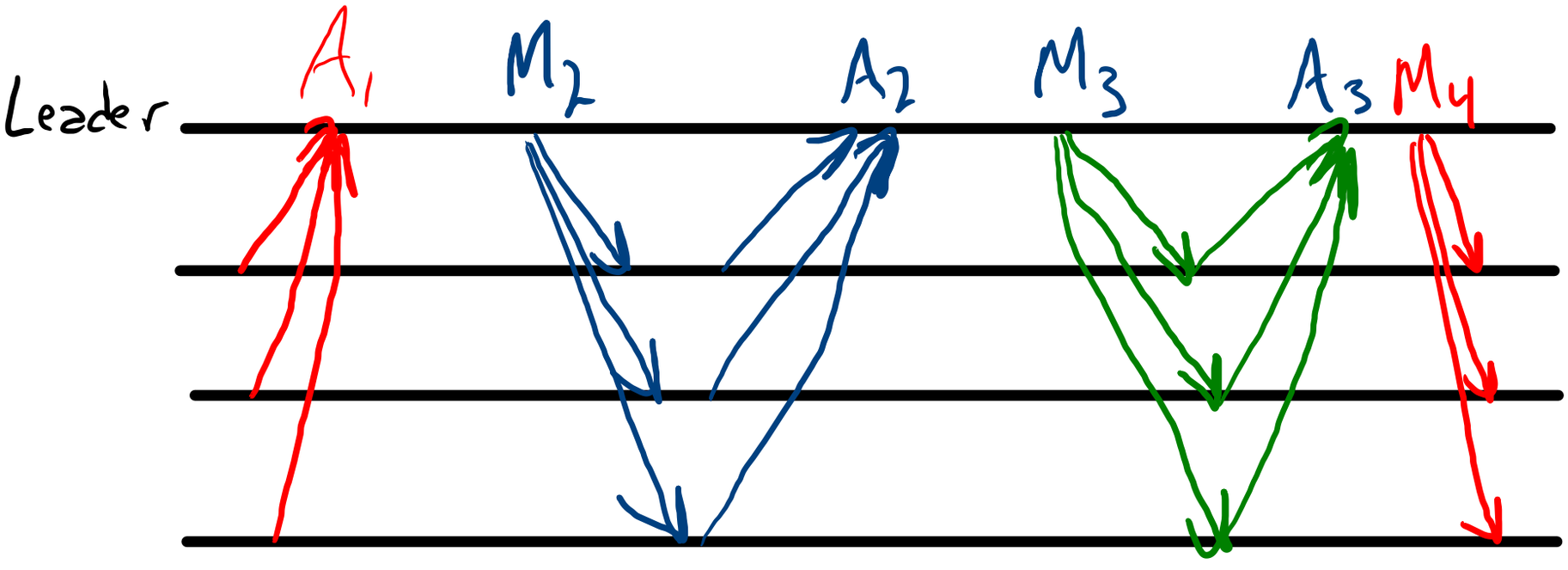
{ H(b_{i-1}), nonce, new transactions }


request
pre-prepare
prepare
commit
reply
C
0
1
2
3
X

$$b' = \{v, H(b), x\}$$



STRAW MAN PROTOCOL



Sate at R_i:

QC: N-f matching signed A2 messages for highest view seen

locked: A "locked" block for which R_i sent A2, or NULL if none locked

{} = unsigned, <> = signed

R_i -> L_v: {A1, v, QC|NULL}

L_v -> R_i: {M2, v, block, QC}

R_i -> L_v: <A2, v, block>

L_v -> R_i: {M3, v, QC2}

R_i -> L_v: <A3, v, block>

L_v -> R_i: {M4, v, QC3}

A2 rules

$b_1 \leftarrow^* b_2$

if block does not extend QC.block

drop

if m.QC.v > lock.v && $\neg$lock$\leftarrow^*$block

if m.QC > QC update QC

set lock$\in$ NULL

$R_i \rightarrow L_v : \{M0, v, QC/NULL\}$

$L_v \rightarrow R_i : \{M1, v, QC/NULL\}$

$R_i \rightarrow L_v : \langle A_1, v, block, QC \rangle$

A0 = NEW-VIEW

A1 = PREPARE

A2 = PRE-COMMIT

M4 = DECIDE

- Commit/externalize when you see N-f signed A3s
- Don't send A3 unless you see N-f signed A2s
- Don't send A2 if its block is incompatible with your locked block
- Lock A2.block when sending A2
- Unlock if you see QC with QC.v > lock.v and ! extends(QC.block, v.block)
- Leader chooses block extending highest QC it knows

Safety of 2-round

w b conflict

N-f A3 msgs from

N-2f honest N = 3f+1

f+1 honest is maj 2f+1

w.v < b.v

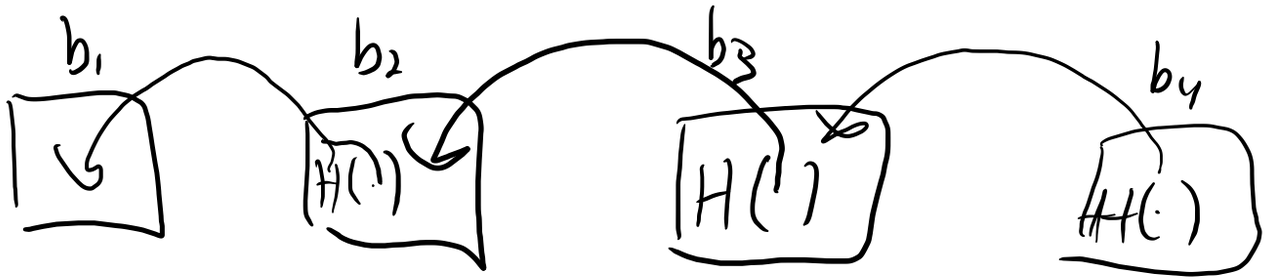
QC N-f A2 msgs N-2f honest

- Still commit/externalize when you see N-f signed A3s
- Don't send A3 unless you see N-f signed A2s
- Don't send A2 unless you see N-f signed A1s
- Don't send A1 if its block is incompatible with your locked block
- Still lock A2.block when sending A2
- But unlock with N-f incompatible higher *A1* messages

When lock?

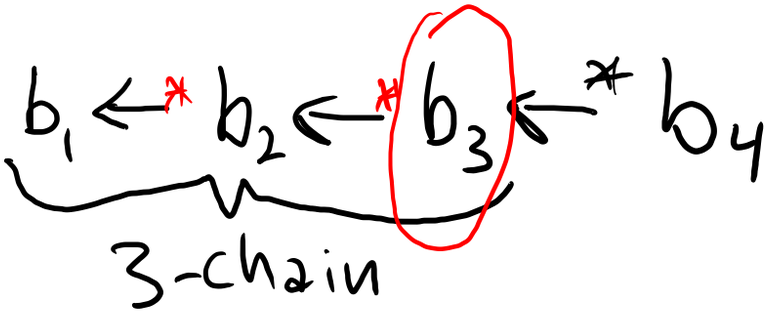
2 round: if you know N-2f honest won't lock conflicting block

3 round: if N-2f honest nodes know that won't lock conflicting block



$\langle A4, b_1, v_1 \rangle$
$\langle A3, b_2, v_2 \rangle$
⋮

Decide b_1
Commit b_2
Pre-com b_3
Prepare b_4



1. Can't commit conflicting blocks in same view

2. A committed block is locked and can't be unlocked.

$w_1 \leftarrow^* w_2 \leftarrow^* w_3 \leftarrow^* w_4$

Pacemaker

ON NEXT SYNC VIEW

LEADER