

Initialise simulator parameters

simulator Run ()

check if cur time > simulation time

Yes

process remaining events except queue new txn or new block

Stop

No

Take event from event queue

Type of event

TXN events

Same as normal blockchain

Mined Block broadcast

Honest

Check Ass 1 design doc

Adversary

Add block in its ~~prev~~ blockchain.
 If in 0 state of selfish, schedule forward block else increase lead by 1.
 Start new mine block

Receive block event

check if block already got

No

Yes

Check Ass 1

Honest

Adversary

Not 0 state

Add block to ~~prev~~ blocks (orphan)

NO

check if received block's parent is in blockchain

Yes

check if block is valid

NO

Add to invalid blocks

Yes (Add to chain)

lead?

Selfish

Forward all blocks from private pool

Forward 1 block from private pool

Update the top block to attack

Stallion

Update the
top block to
attach, update txns
if longest branch change

0

lead?

≥ 2

Release 1
block

Schedule
forward block
for all private block

