Lecture 7.

Liveness of Bitcoin

← longest chain Protocol

Last lecture: Safety of longest chain protocol.

means that once a block is confirmed (e.g. k-deep) then the prob. of deconfirmation is very small.

→ Safety is an important security property

→ but what if no blocks get into the ledger!

→ or blocks get in but some (honest) transactions don't.

Liveness is an important security property

→ focus of this lecture.

Observation 1: The longest chain protocol cannot deadlock.

— mining operation is very democratic & even a single honest miner with tiny hash power will eventually succeed mining

Observation 2: But the ledger is made up of blocks on the longest chain. It could happen that all blocks on the longest chain are adversarial.

Chain growth (CG): rate of growth of the longest chain.

Ob 1: $CG > 0$.

honest hash power fraction

- adv. stays silent $CG = \widetilde{(1-\beta)\lambda}$

$1+((1-\beta)\lambda\Delta$ ← network delay.

$\frac{1}{\lambda}$ = inter block mining & access time

- adv. acts honest.

$$CG = \frac{(1-\beta)\lambda}{1+(1-\beta)\lambda\Delta} + \beta\lambda .$$

- claim: $\boxed{CG \geq \frac{(1-\beta)\lambda}{1+(1-\beta)\lambda\Delta}}$

Ob2: Chain Quality: (CQ)

$$CQ = \frac{\#\text{ of honest blocks in the longest chain}}{\#\text{ of all blocks in}}$$

the longest chain.

really we need $CQ > 0$ for liveness

$$CQ \geq \frac{CG \cdot \lambda - \beta\lambda \cdot \lambda}{CG \cdot \lambda}$$

$$\boxed{CQ \geq \frac{CG - \beta\lambda}{CG}}$$

$$\boxed{\frac{(1-\beta)\lambda}{1+(1-\beta)\lambda\Delta} \geq \beta\lambda} \quad \text{for } CQ > 0.$$

↑ exact same condition for safety.

Turns out the condition above is also necessary for liveness. → selfish mining

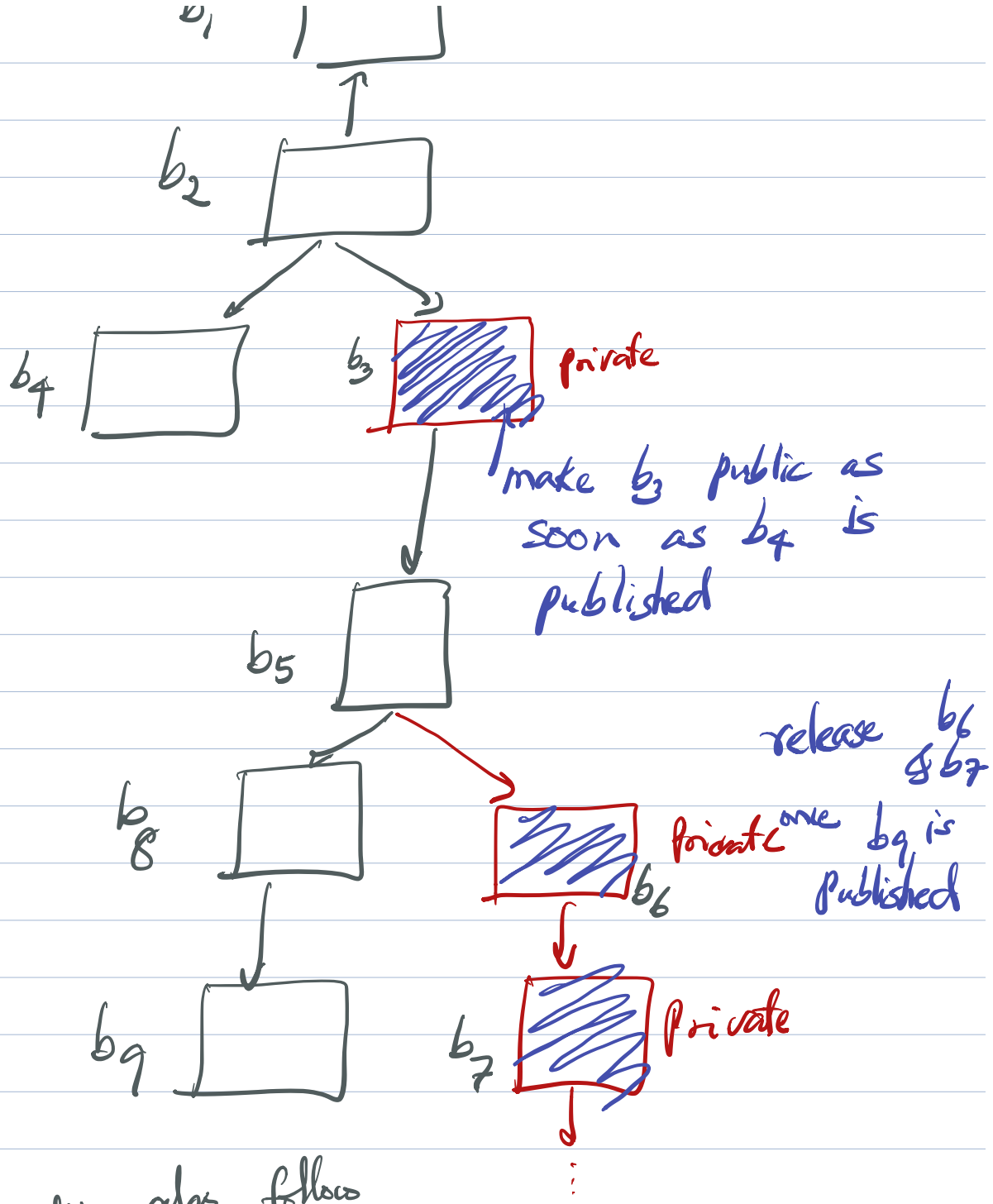
Same / analogous as safety: there private attack was fatal.

Selfish - Mining Attack:

(1) Adv. always mines on the tip of the longest chain. (same as honest)

They keep successfully mined blocks **private**.

(2) Adv. publishes/broadcasts a previously mined block exactly when an honest block at the same level appears.



$$1-\beta \geq CQ \geq \frac{(1-\beta)\lambda}{1+(1-\beta)\lambda\Delta} - \beta\lambda$$

1 ↑ $\frac{(1-\beta)\lambda}{1+(1-\beta)\lambda\Delta}$

Quantifying how live the protocol is

Quantify the fairness

The most fair rewards distribution occurs when # of honest blocks on longest chain $\propto$ honest hash power.

$= (1-\beta)$.

i.e., $CQ = 1-\beta$.

not happening in the longest chain protocol (e.g. because of selfish mining).

Question: how to "modify" the

longest chain protocol so that optimal CQ is obtained?

Fruitchains: "rewards".

main idea: separate tx's (& their rewards) from blocks in the longest chain.

Two types of blocks.

Tx block.

regular block. ~ [only the header] essentially empty

(1) how to relate these 2 types of blocks?

(2) how to do PoW for both

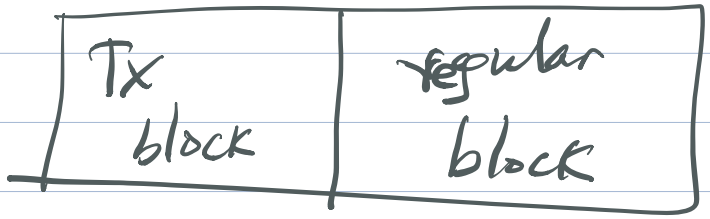
blocks simultaneously ?

Tcritical.

Key crypto idea:

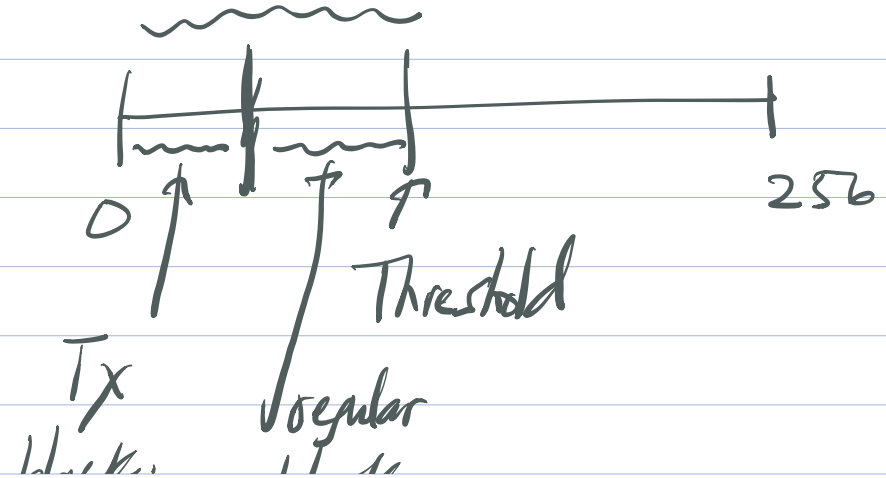
2:1 mining or Sortition.

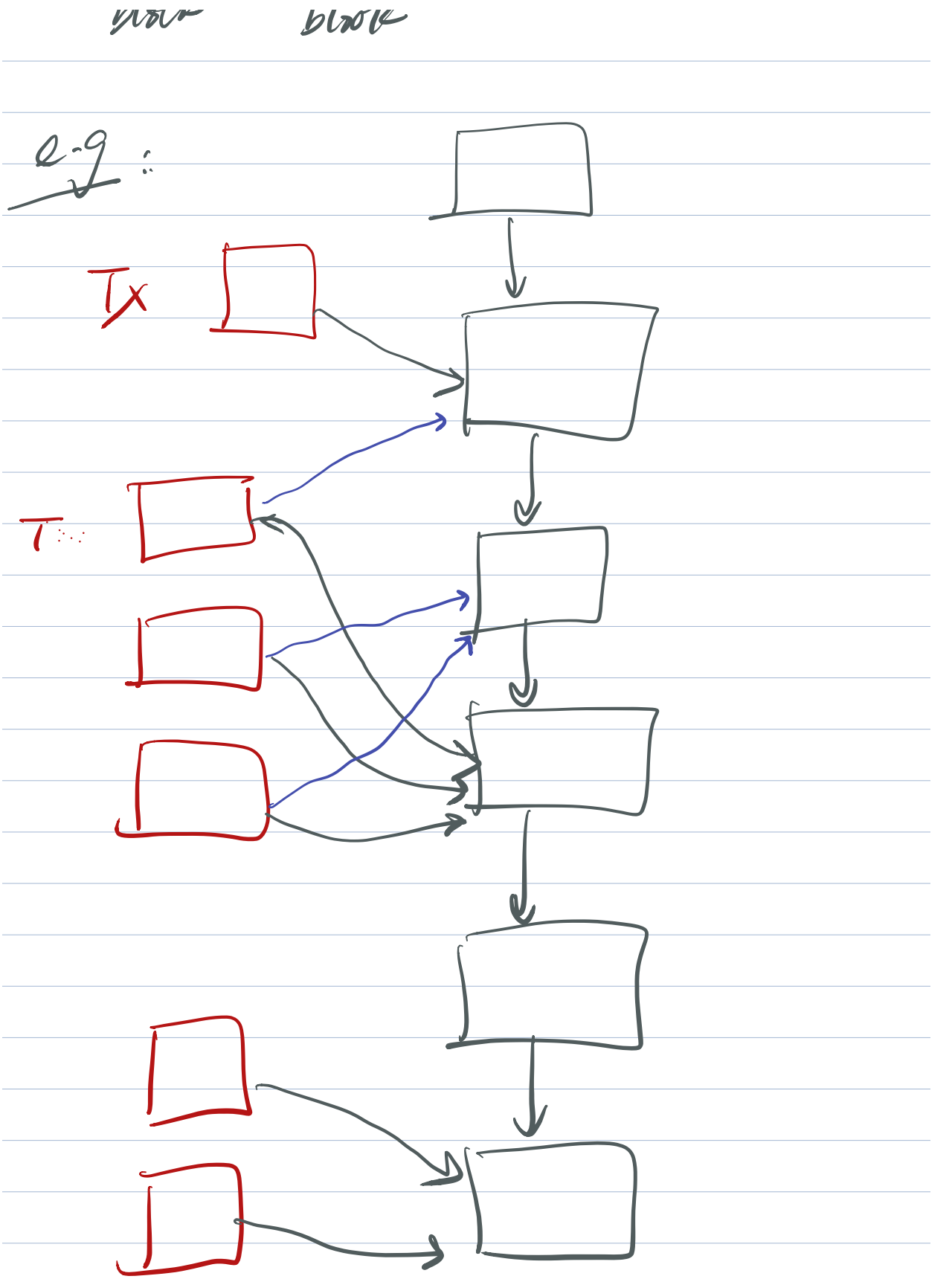
generate a super block:



mine on super block.

hash (super block) < threshold.




e.g. :
Tx
T...

Important fact: # of tx blocks referred to by a honest miner $\propto$ hash power of the miner; not how often the honest blocks are in the longest chain.

$\Rightarrow$ perfect chain quality.