SNS COLLEGE OF TECHNOLOGY

Coimbatore-35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A++' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

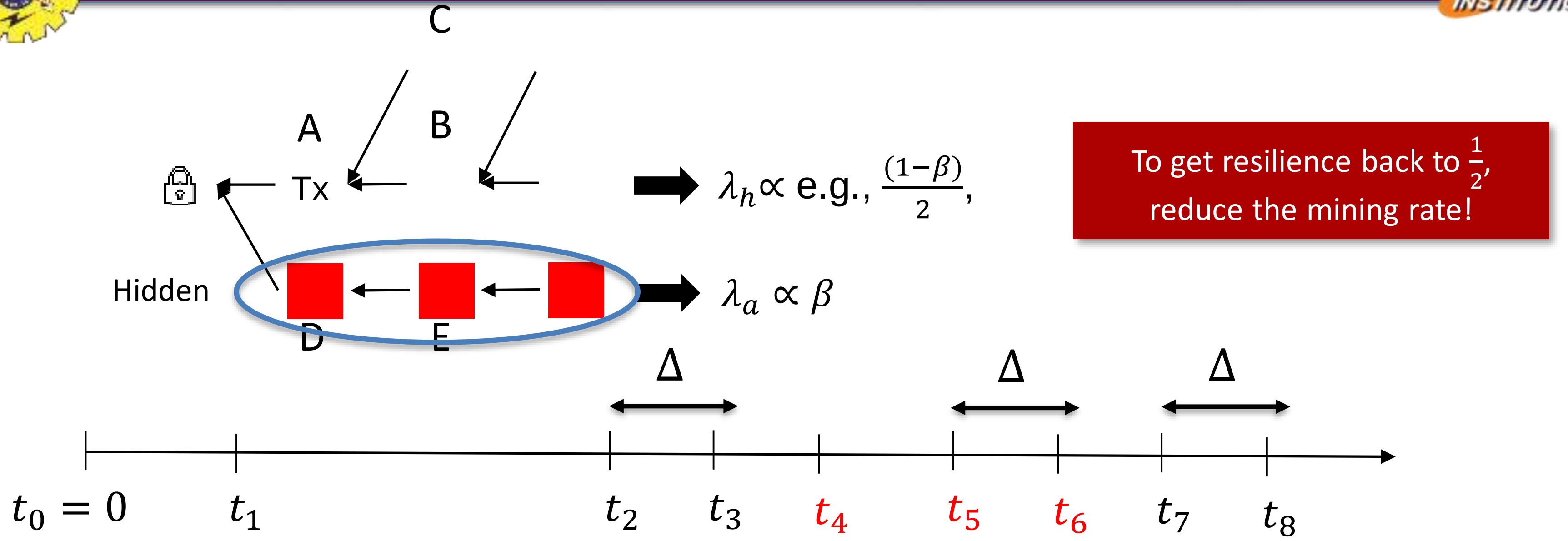
DEPARTMENT OF INFORMATION TECHNOLOGY

BLOCK CHAIN AND CRYPTOCURRENCY

IV YEAR - VII SEM

UNIT 3 - DISTRIBUTED CONSENSUS & BLOCK CHAIN APPLICATIONS

Forking



Multiple honest blocks at the same height due to network delay.
Adversary's chain grows at rate proportional to (shown by $\propto$) β!
Honest miners' chain grows at rate less than $1-\beta$ because of forking!

Now, adversary succeeds if $\beta \geq \frac{(1-\beta)}{2}$, which implies $\beta \geq \frac{1}{3}$!!

Reminder for SMR Security

Let's recall the security definition for state machine replication (SMR) protocols. Let ch_t^i denote the confirmed (i.e., k-deep) of a client i at time t.

Safety (Consistency):

- For any two clients i and j, and times t and s: $\boldsymbol{ch_t^i} \preccurlyeq \boldsymbol{ch_s^j}$ (prefix of) or vice versa, i.e., chains are consistent.

No double spend

Liveness:

- If a transaction tx is input to an honest miner at some time t, then for all clients i, and times $s \geq t + T_{conf}$: $tx \in \boldsymbol{ch_s^i}$.

No censorship

Security Theorem

Theorem: If $\beta < 1/2$, there exists a small enough mining rate $\lambda(\Delta, \beta) = \lambda_a + \lambda_h$ such that Bitcoin satisfies safety and liveness except with error probability $\epsilon = e^{-\Omega(k)}$ under synchronous network (recall that k is used in the k deep confirmation rule).

- $e^{-\Omega(k)}$ is the error probability for confirmation.
- Latest result for bounding the error probability as a function of k:

$$\epsilon \leq \left(2 + 2\sqrt{\frac{1-\beta}{\beta}}\right)\left(4\beta(1-\beta)\right)^k$$

- We say 'confirmation' instead of finalization because when you *confirm* a block or transaction, you *confirm* it with an error probability…
- …unlike *finalizing* a block where there is no error probability*.

The Bitcoin Backbone Protocol: Analysis and Applications (2015)
Analysis of the Blockchain Protocol in Asynchronous Networks (2016)
Analysis of Nakamoto Consensus (2019)
Everything is a Race and Nakamoto Always Wins (2020)
Bitcoin's Latency–Security Analysis Made Simple (2022)

Security Theorem

Theorem: If $\beta < 1/2$, there exists a small enough mining rate $\lambda(\Delta, \beta) = \lambda_a + \lambda_h$ such that Bitcoin satisfies safety and liveness except with error probability $\epsilon = e^{-\Omega(k)}$ under synchronous network (recall that k is used in the k deep confirmation rule).

- $e^{-\Omega(k)}$ is the error probability for confirmation.
- Latest result for bounding the error probability as a function of k:

$$\epsilon \leq \left(2 + 2\sqrt{\frac{1-\beta}{\beta}}\right)\left(4\beta(1-\beta)\right)^k$$

- We say ‘confirmation’ instead of finalization because when you *confirm* a block or transaction, you *confirm* it with an error probability…
- …unlike *finalizing* a block where there is no error probability*.

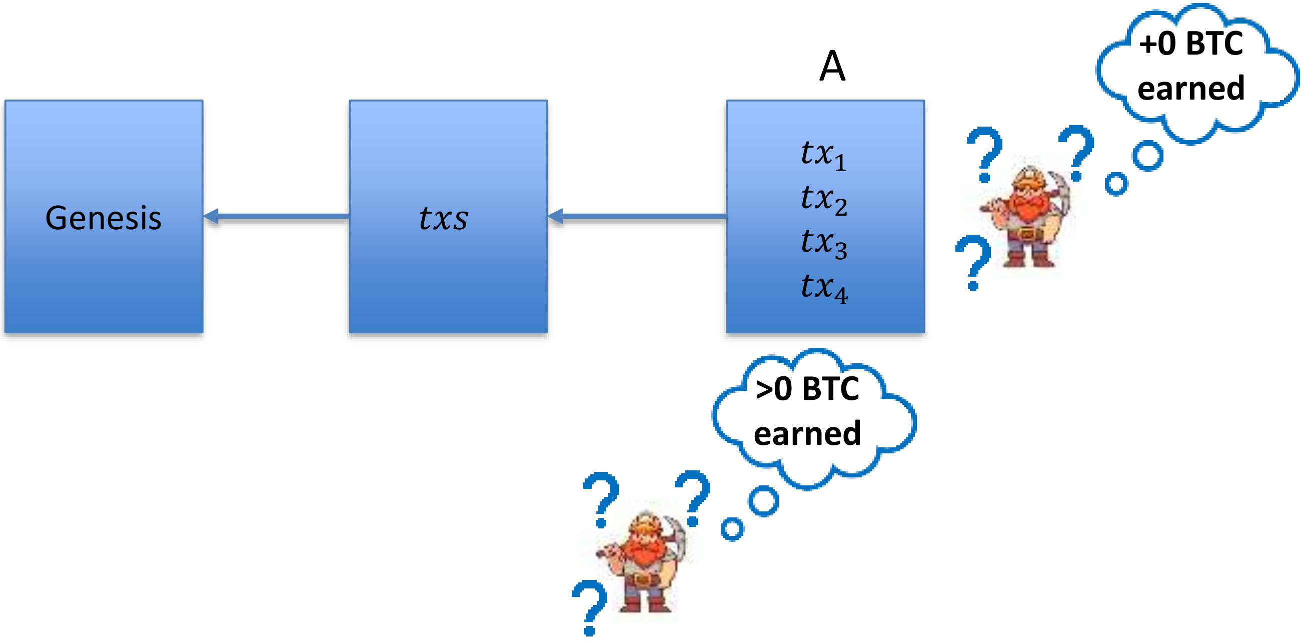
The Bitcoin Backbone Protocol: Analysis and Applications (2015)
Analysis of the Blockchain Protocol in Asynchronous Networks (2016)
Analysis of Nakamoto Consensus (2019)
Everything is a Race and Nakamoto Always Wins (2022)
Bitcoin’s Latency–Security Analysis Made Simple (2022)

Now, we see why Bitcoin has 1 block every 10 minutes, instead of 1 block every second…

Proof of the Security Theorem

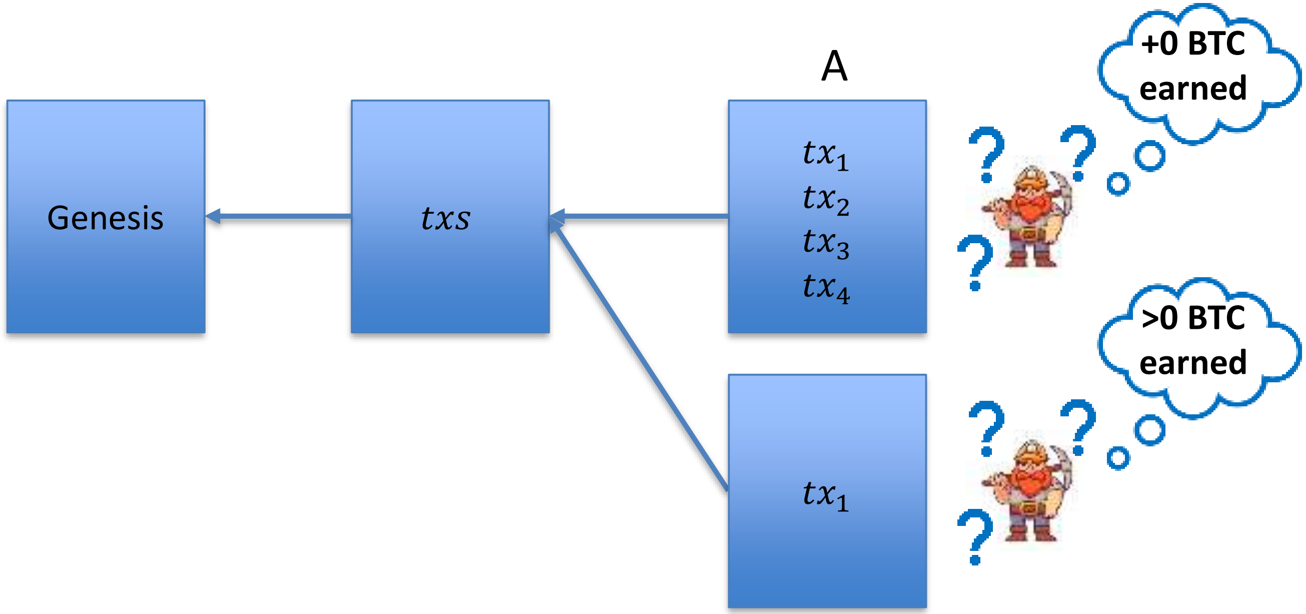
Case 1

Would $\beta < 1/2$ hold in practice?



Transaction fees
(paid to the miner):
tx_1: 4 BTC
tx_2: 3 BTC
tx_3: 2 BTC
tx_4: 1 BTC

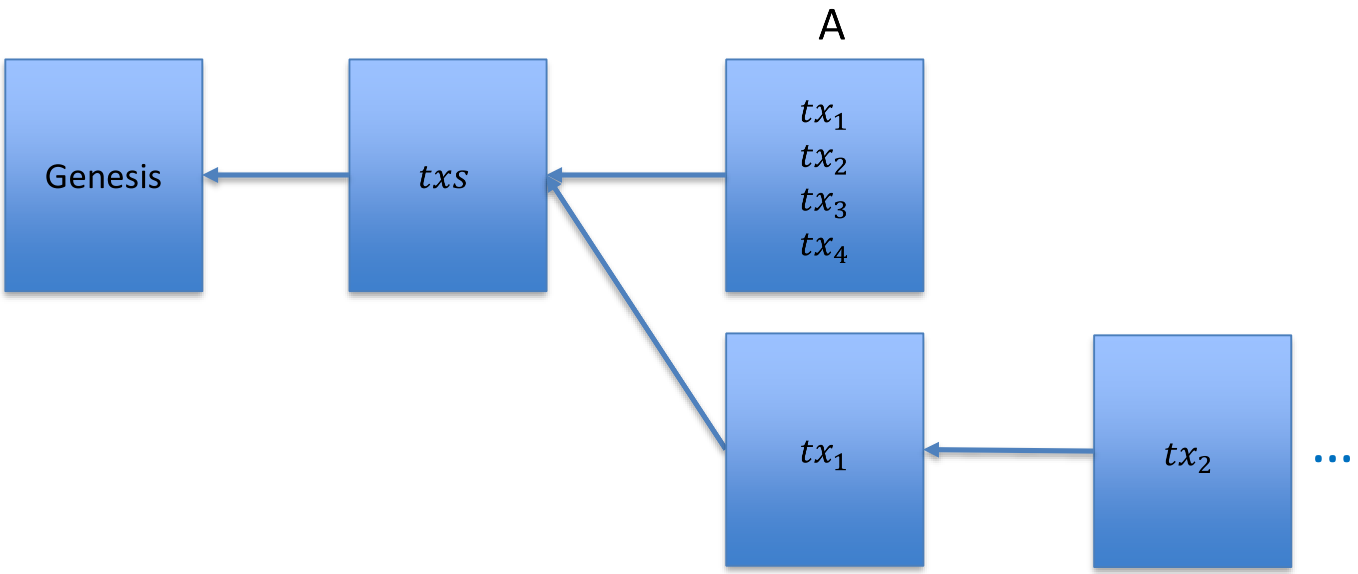
Would $\beta < 1/2$ hold in practice?



Transaction fees
(paid to the miner):

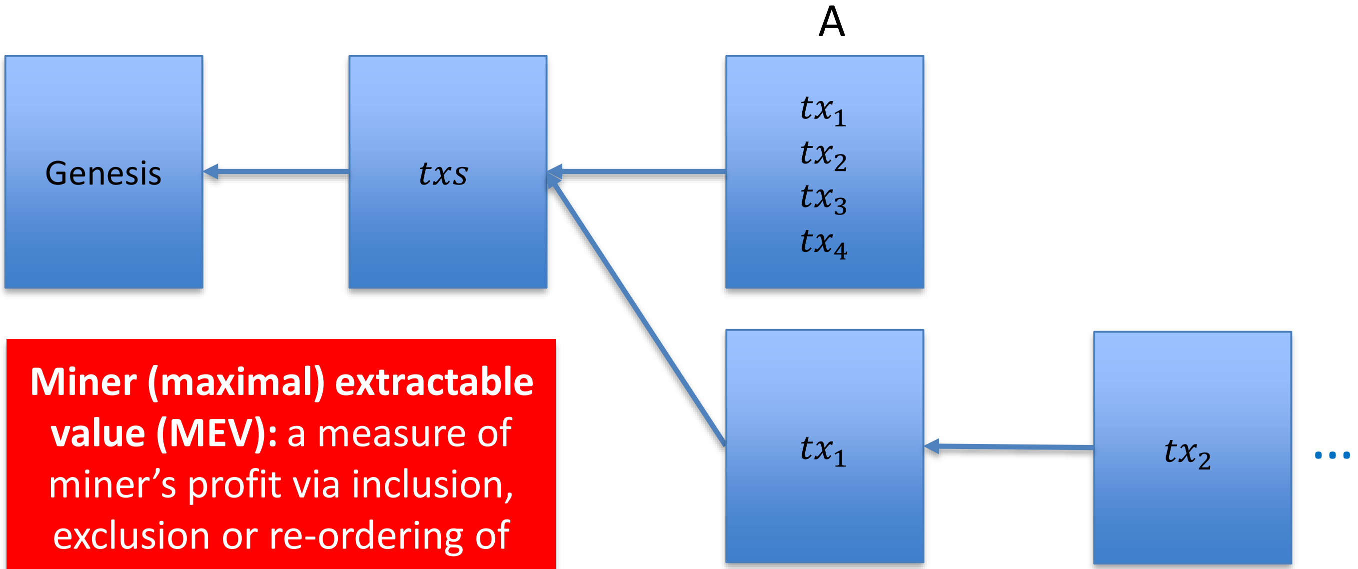
tx_1: 4 BTC
tx_2: 3 BTC
tx_3: 2 BTC
tx_4: 1 BTC

Would $\beta < 1/2$ hold in practice?



Transaction fees
(paid to the miner):
tx_1: 4 BTC
tx_2: 3 BTC
tx_3: 2 BTC
tx_4: 1 BTC

Would $\beta < 1/2$ hold in practice?



Transaction fees
(paid to the miner):
tx_1: 4 BTC
tx_2: 3 BTC
tx_3: 2 BTC
tx_4: 1 BTC

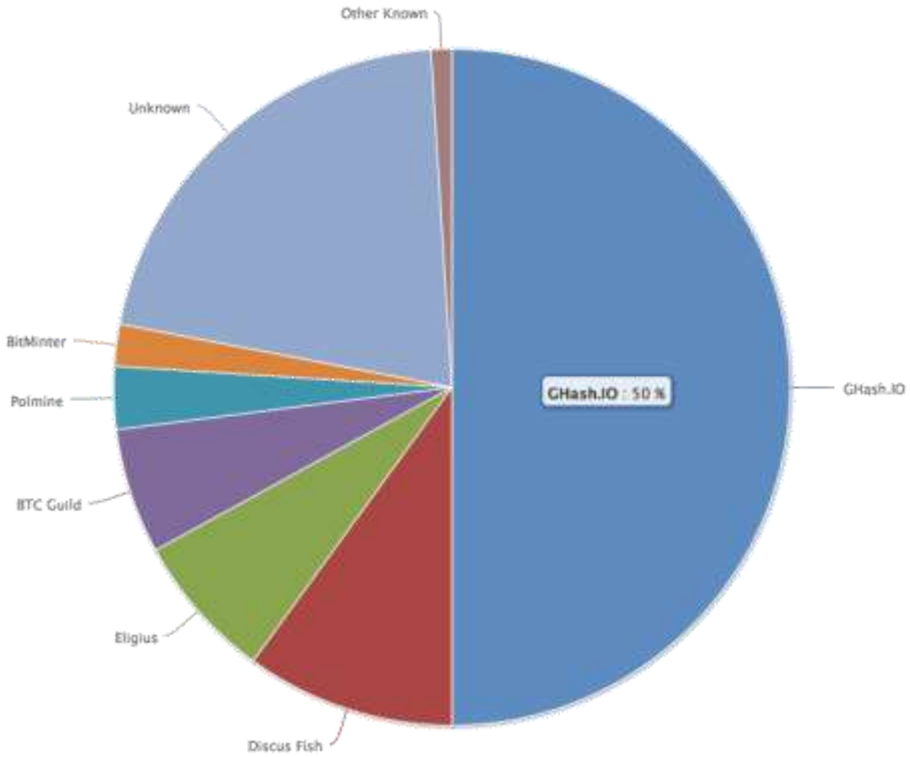
Miner (maximal) extractable value (MEV): a measure of miner's profit via inclusion, exclusion or re-ordering of transactions within its block

- Miners have incentive to violate the protocol!
- Can lead to double spends!

Need to think about incentives!!

MEV gives even more incentive to violate the protocol!!

No Attacks on Bitcoin?



Ghash.IO had >50% in 2014

- Gave up mining power

Why are visible attacks not more frequent?

Miners care about the Bitcoin price?

- Not a valid argument.
- They can 'short' the chain for profit!

Might not always be rational to attack.

No guarantees for the future!

Is Bitcoin the Endgame?

Bitcoin provides Sybil resistance and dynamic availability.

Is it the Endgame for consensus?

No!

Bitcoin is secure only under synchrony and loses security during periods of asynchrony.

It *confirms* blocks with an error probability depending on *k*, i.e., blocks are not finalized.

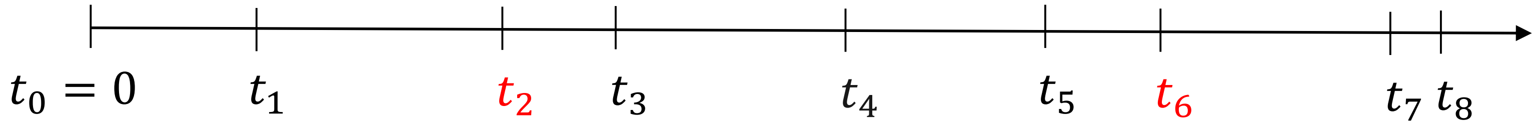
Energy consumption?

Next lecture: low-energy consensus using proof-of-stake

Optional: Security Proof

Loner block:

- An honest block such that no other honest block is mined within Δ time of the loner block.

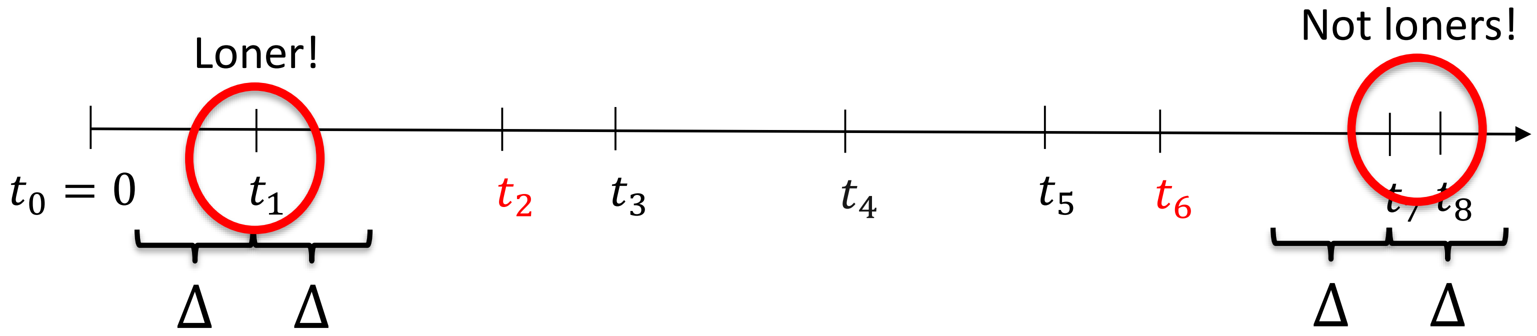


Analysis of Nakamoto Consensus (2019)
The Sleepy Model of Consensus (2016)

Optional: Security Proof

Loner block:

- An honest block such that no other honest block is mined within Δ time of the loner block.



Length of the shortest chain among the longest chains observed by the clients at time t:

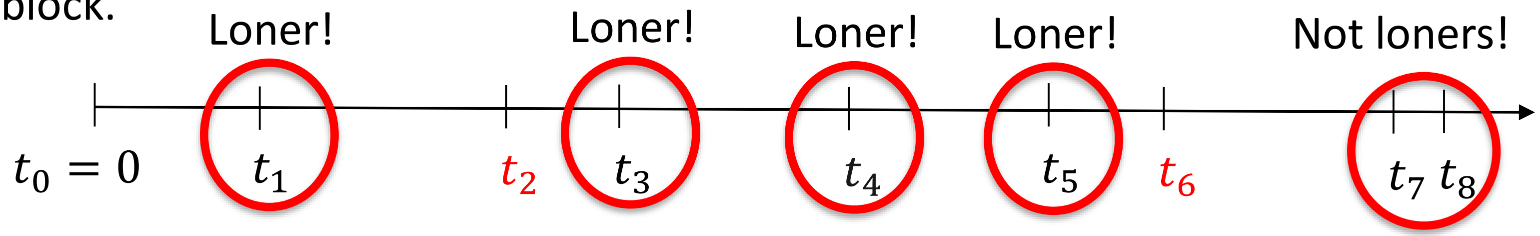
$$L(t)$$

Analysis of Nakamoto Consensus (2019)
The Sleepy Model of Consensus (2016)

Optional: Security Proof

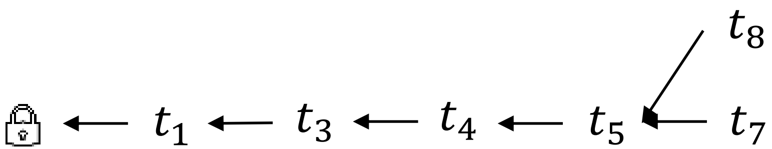
Loner block:

- An honest block such that no other honest block is mined within Δ time of the loner block.



Lemma: For any $s > t$, $L(s) - L(t) \geq$ "number of loners mined in the interval $(t + \Delta, s - \Delta]$".

Proof sketch: Each loner increases the length of the longest chains observed by the clients by one block. For instance;

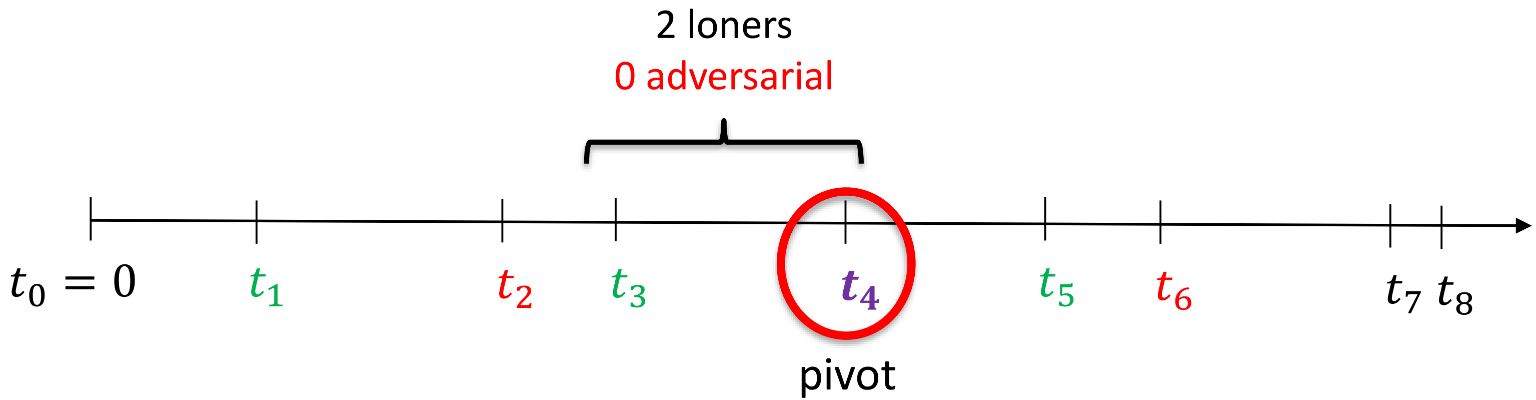


Analysis of Nakamoto Consensus (2019)
The Sleepy Model of Consensus (2016)

Optional: Security Proof

Pivot block:

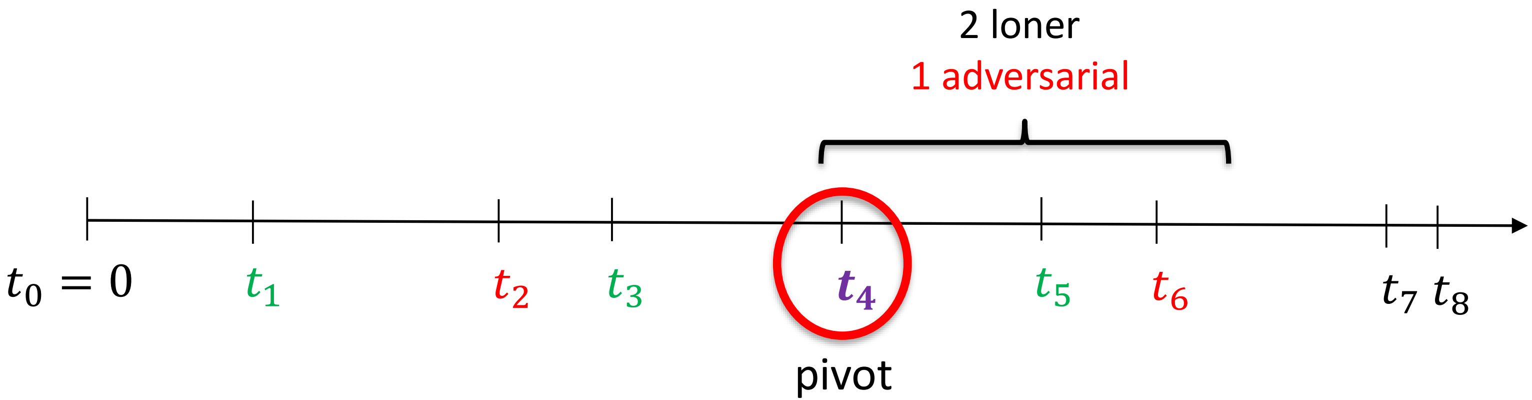
- In any interval covering the mining time of the pivot block, more loner blocks are mined than adversarial blocks.
- Pivot block is a loner.



Optional: Security Proof

Pivot block:

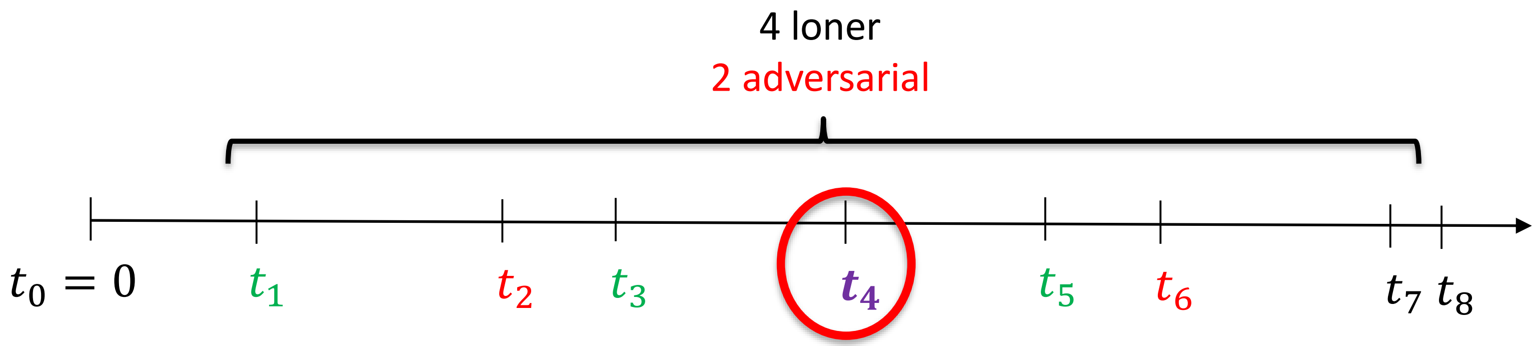
- In any interval covering the mining time of the pivot block, more loner blocks are mined than adversarial blocks.
- Pivot block is a loner.



Optional: Security Proof

Pivot block:

- In any interval covering the mining time of the pivot block, more loner blocks are mined than adversarial blocks.
- Pivot block is a loner.



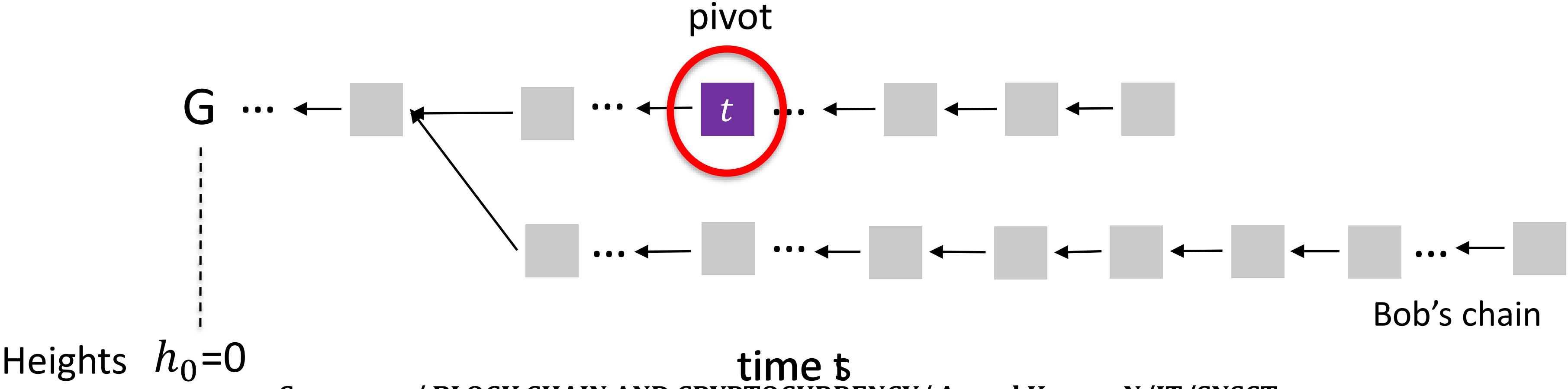
Theorem: If $\beta < 1/2$, there exists a small enough mining rate $\lambda(\Delta, \beta)$ such that any time interval of T have a pivot except with probability $e^{-\Omega(\sqrt{T})}$.

Proof: Probability theory

Optional: Security Proof

Theorem: Suppose a block mined at time t is a pivot. Then, the pivot block is on every (longest) chain held by any client at all times $\geq t$.

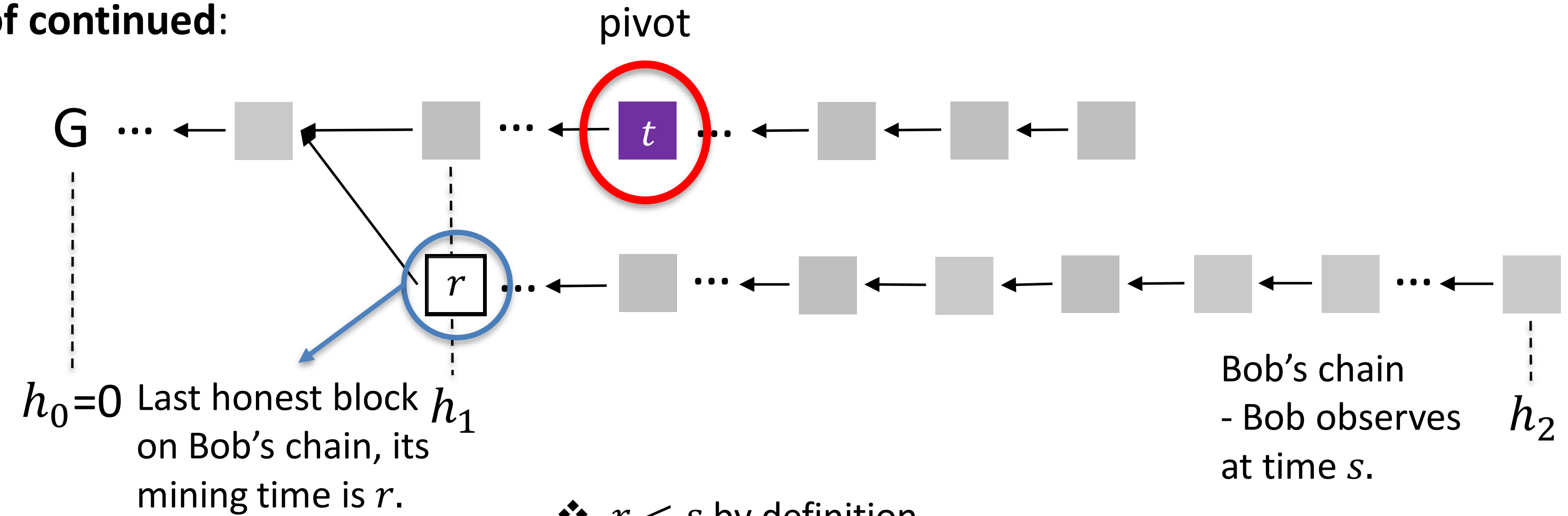
Proof: For contradiction, suppose there exists a minimum time $s \geq t$ such that a client Bob holds a chain conflicting with the pivot block.



Optional: Security Proof

Theorem: If a client holds a chain containing a pivot block, then no client can hold a chain conflicting with the pivot block after the pivot block is mined.

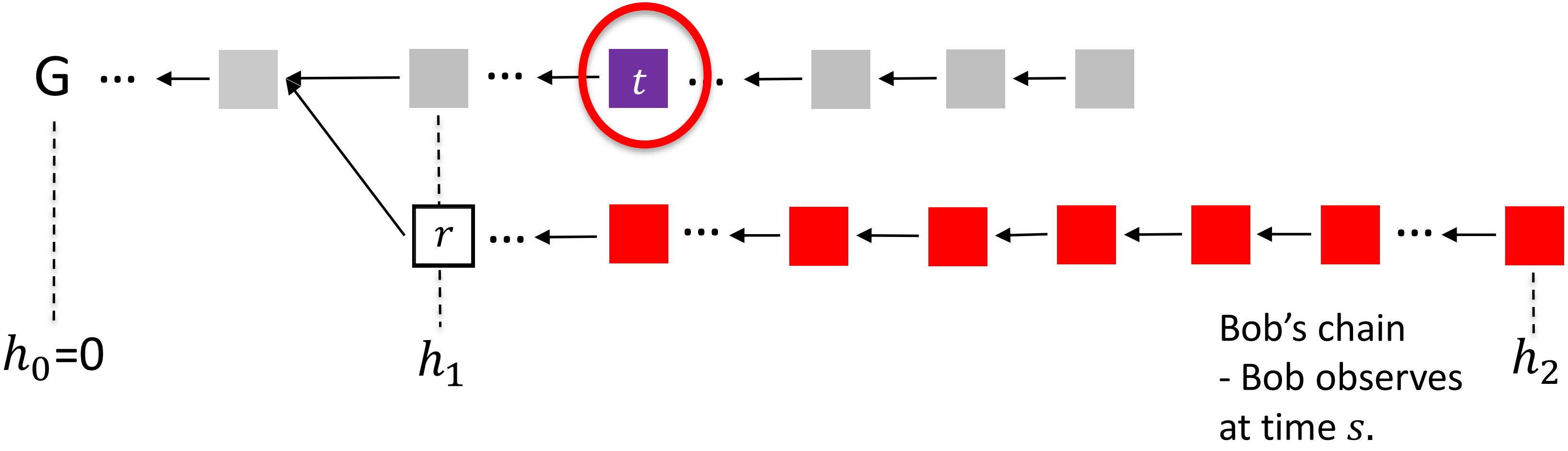
Proof continued:



- ❖ $r < s$ by definition.
- ❖ $r < t$ because otherwise s is not the first time a conflicting chain is held by a client or honest miner.

Optional: Security Proof

Proof continued:

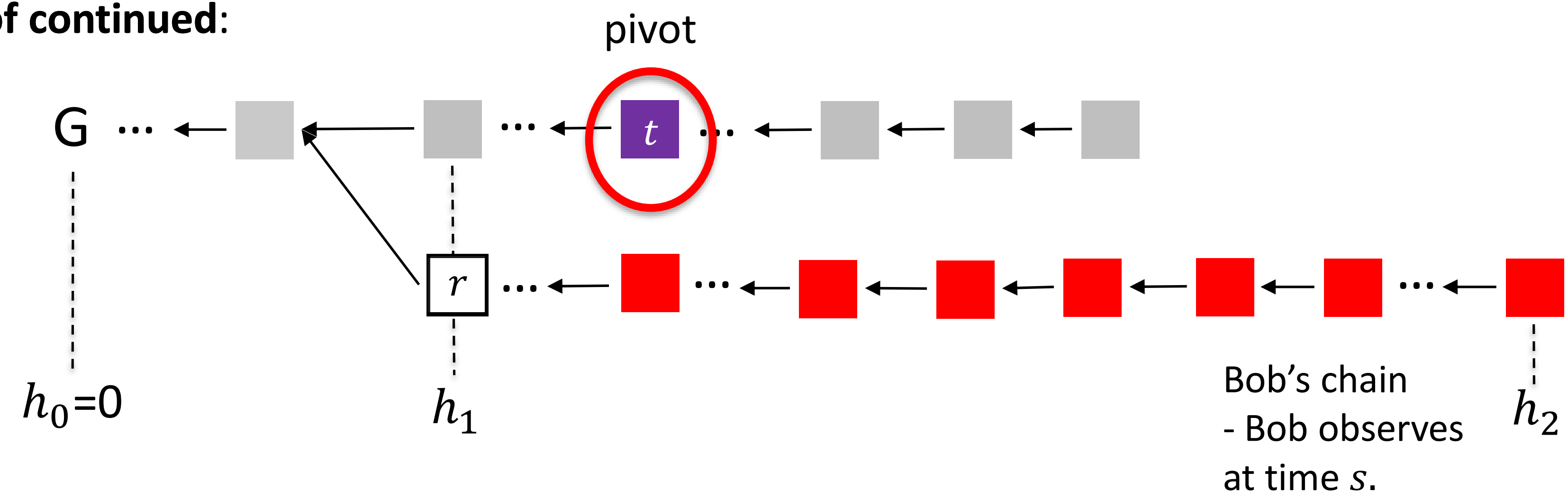


- $h_2 - h_1 <$ "blocks mined by the adversary in the interval $(r, s]$"
- length of the shortest 'longest chain' held by any client at time r, $L(r) \leq h_1$
- length of Bob's chain at time s, $h_2 \geq L(s)$

Hence, $h_2 - h_1 \geq L(s) - L(r) \geq$ "number of loners mined in the interval $(r + \Delta, s - \Delta]$" by the lemma.

Optional: Security Proof

Proof continued:



Finally, "blocks mined by the adversary in the interval $(r, s]$" $> h_1 - h_2$

$h_1 - h_2 \geq L(s) - L(r) \geq$ "number of loners mined in the interval $(r + \Delta, s - \Delta]$".

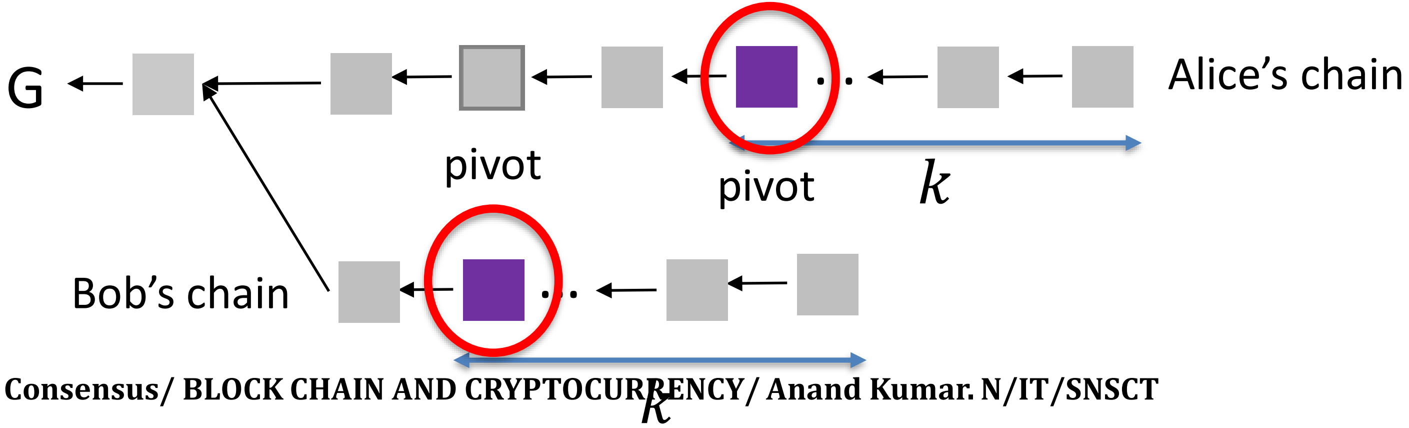
In the interval $(r, s]$ covering t, more adversary blocks are mined than loners!

Contradiction with the definition of pivot!!

Optional: Security Proof

Proof Sketch of Liveness: The pivot is mined by an honest miner and contains all transactions input to the honest miners. Since it is on all chains held by all clients at all times, liveness is satisfied.

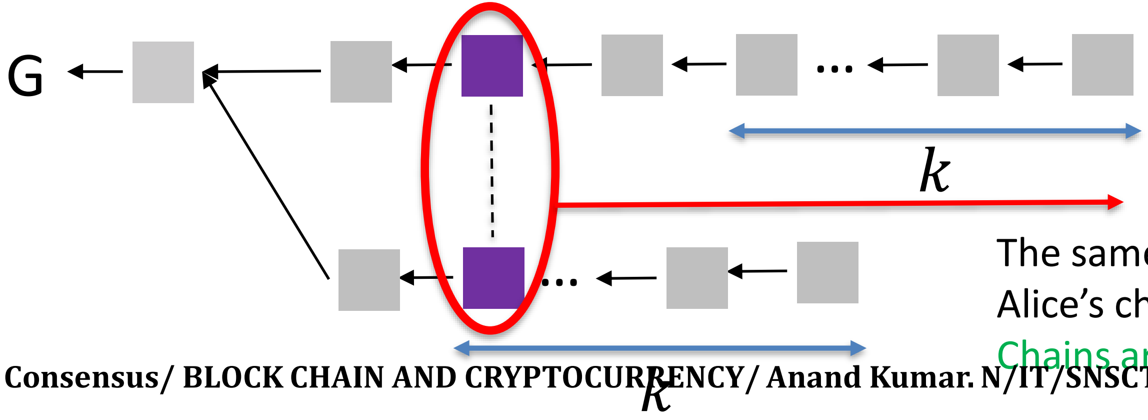
Proof Sketch of Safety: Consider two clients that confirm two chains after chopping off the last k blocks on their chains. One of the last k blocks is a pivot on both chains except with probability $e^{-\Omega(\sqrt{k})}$ (follows from probability theory). Thus,



Optional: Security Proof

Proof Sketch of Liveness: The pivot is mined by an honest miner and contains all transactions input to the honest miners. Since it is on all chains held by all clients at all times, liveness is satisfied.

Proof Sketch of Safety: Consider two clients that confirm two chains after chopping off the last k blocks on their chains. One of the last k blocks is a pivot on both chains except with probability $e^{-\Omega(\sqrt{k})}$ (follows from probability theory). Thus,



Pivots:

The same block appears in Alice's chain by the Theorem.

Chains are consistent!!