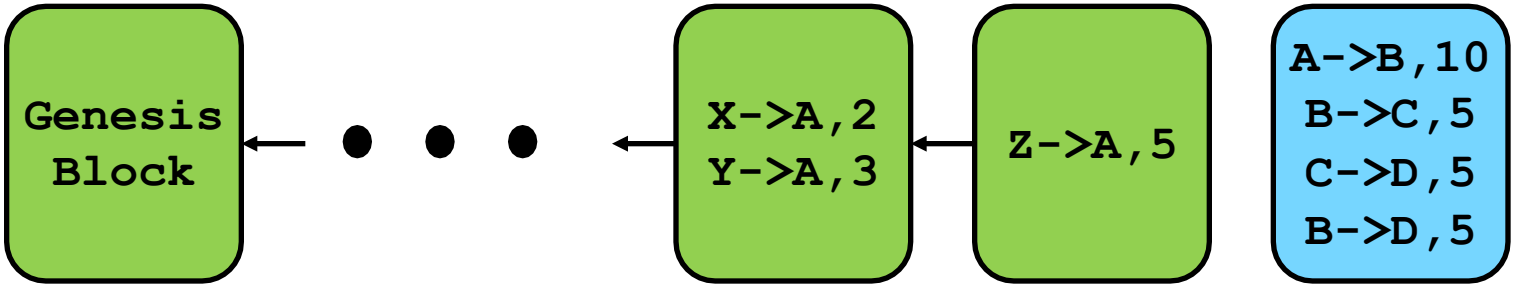
LCA

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Majority is not Enough: Bitcoin Mining is Vulnerable

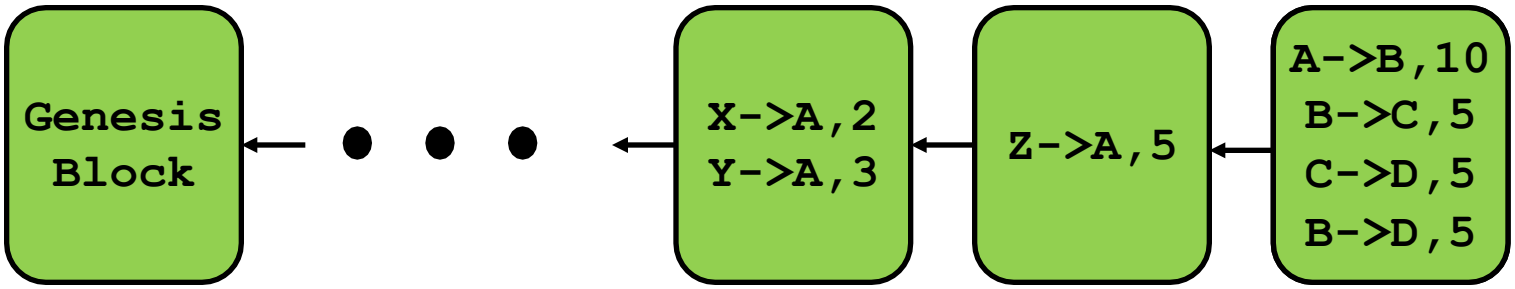
Paper by Ittay Eyal and Emin Gün Sirer (Cornell)

Bitcoins and Blockchains



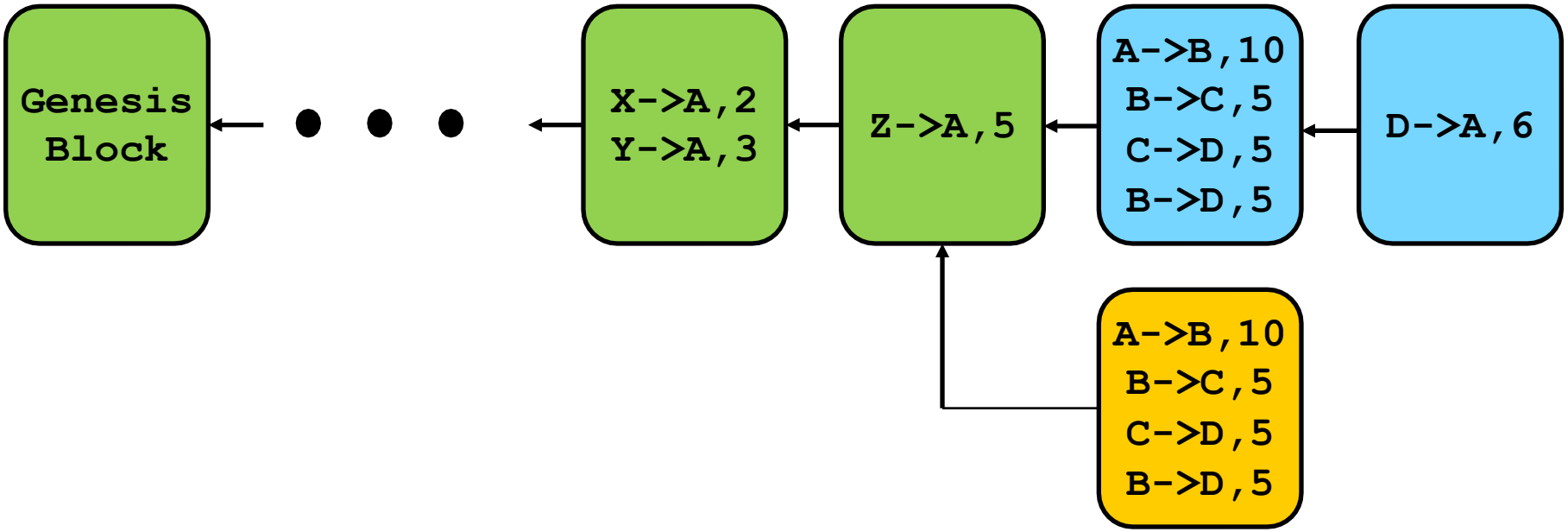
- Bitcoin = distributed, decentralized crypto-currency.
- Bitcoin clients make transactions, that are signed (using the clients' secret keys), recorded in a block that is appended to a global public ledger.
- Blockchain = global public ledger maintained at all bitcoin nodes.
- Client A owns x Bitcoins at time t if in the prefix of the blockchain at time up to time t, balance of transactions to A = x.
- Immutable: impossible to change the past.

Bitcoins and Blockchains



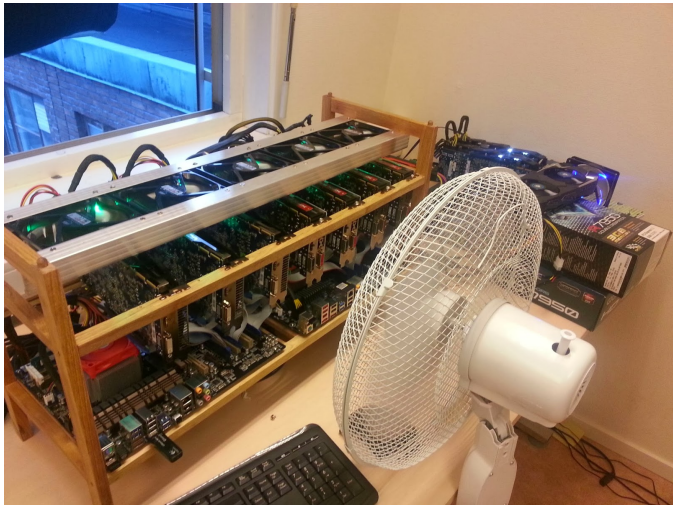
- Miners maintain Blockchain:
  - Miner solves a crypto-puzzle involving hash(last previous block) + hash(current block) = "mining the current block".
  - Miner publishes the mined block by gossiping it to the bitcoin network.
  - The mined block is appended to the chain.
  - Miner gets a reward in bitcoin for mining the block.

Bitcoins and Blockchains



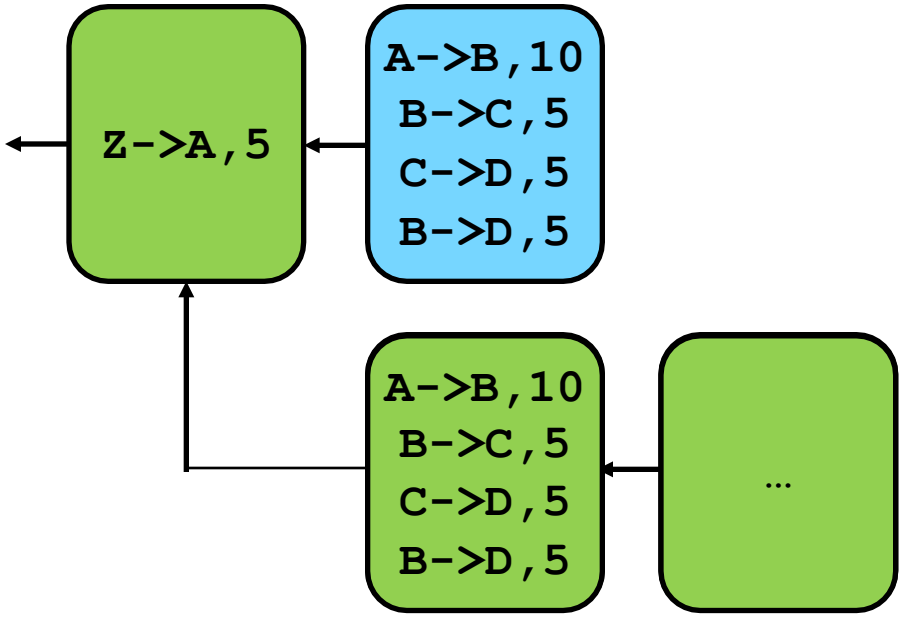
- Difficulty of the crypto-puzzle such that it takes ~10 min on average for a new block to appear.
- Dissemination delays are ~ a few seconds.
- Forking is possible but rare. Should be avoided to maintain a unique global public, totally ordered ledger.
- Rule: mine on the longest (most difficult) chain, prune others.

Pooling



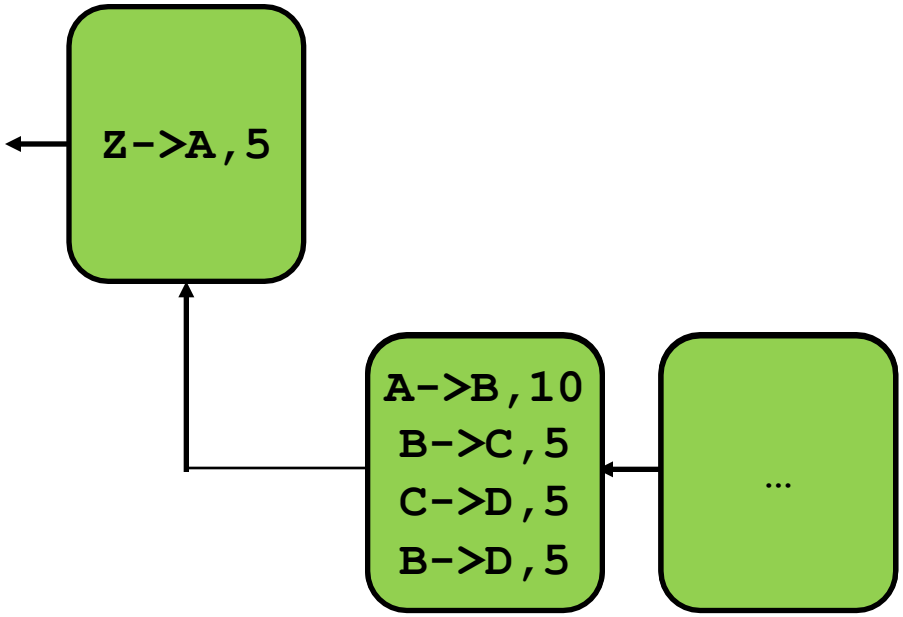
- Difficulty of the crypto-puzzle such that it takes ~10 min on average for a new block to appear.
- Probability to solve a block proportional to computational power.
- A single home miner with ASIC will need years to mine a block.
- Miners pool together and share revenues when one miner succeed.
- What if a pool is selfish?

Selfish Mining by Dishonest Pool



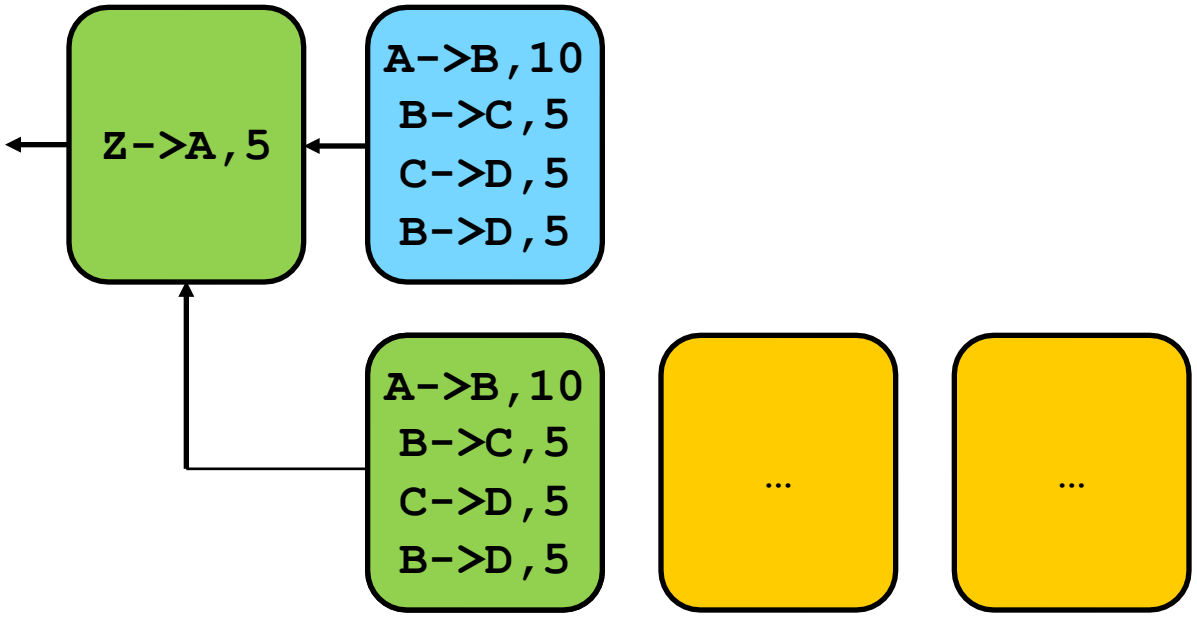
- Pool keeps its discovered blocks private, forcing forking.
- Honest nodes mine on public branch.
- Dishonest pool mines on its own private branch.
- When one block is discovered by honest nodes, pool publishes two private blocks if it is ahead of at least two blocks
- Pool gets bitcoins reward for two blocks, public branch is pruned.

Selfish Mining by Dishonest Pool: Lead = 2



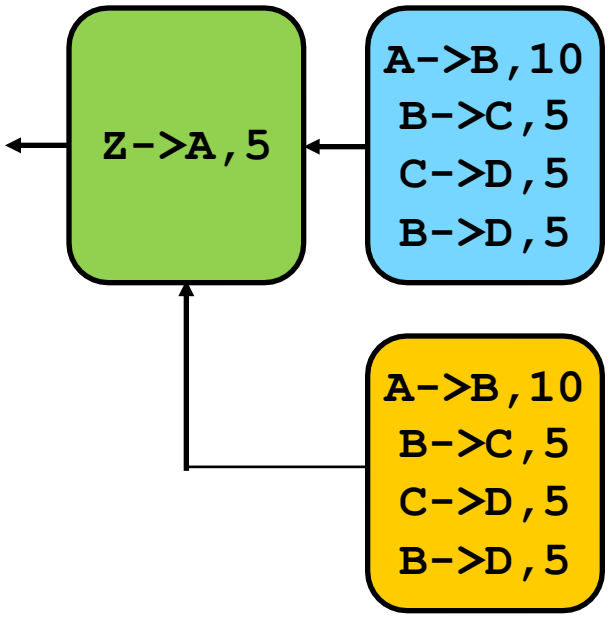
- Pool keeps its discovered blocks private, forcing forking.
- Honest nodes mine on public branch.
- Dishonest pool mines on its own private branch.
- When one block is discovered by honest nodes, pool publishes two private blocks if it is ahead of at least two blocks
- Pool gets bitcoins reward for two blocks, public branch is pruned.
- Only 1 public global chain just after rewards received, start over.

Selfish Mining by Dishonest Pool: Lead by >2



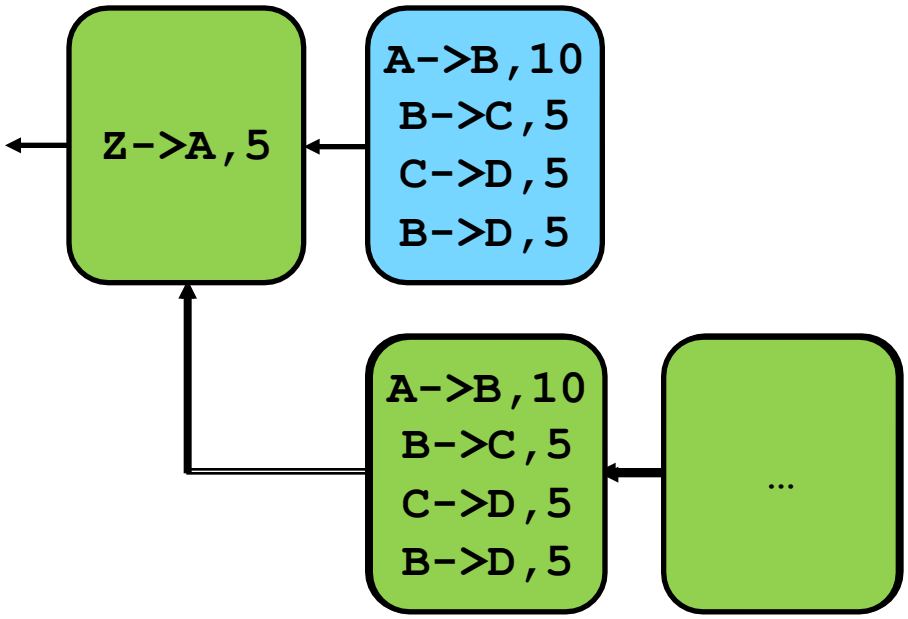
- When the pool has a lead of more than 2 blocks, it continues mining on the private chain, keeping it private.
- It publishes the first private block as soon as one block is discovered by honest nodes.
- Pool will get bitcoins reward for 1 block (when it will be kept in the global chain, after other blocks are appended).

Selfish Mining by Dishonest Pool : Lead by 1



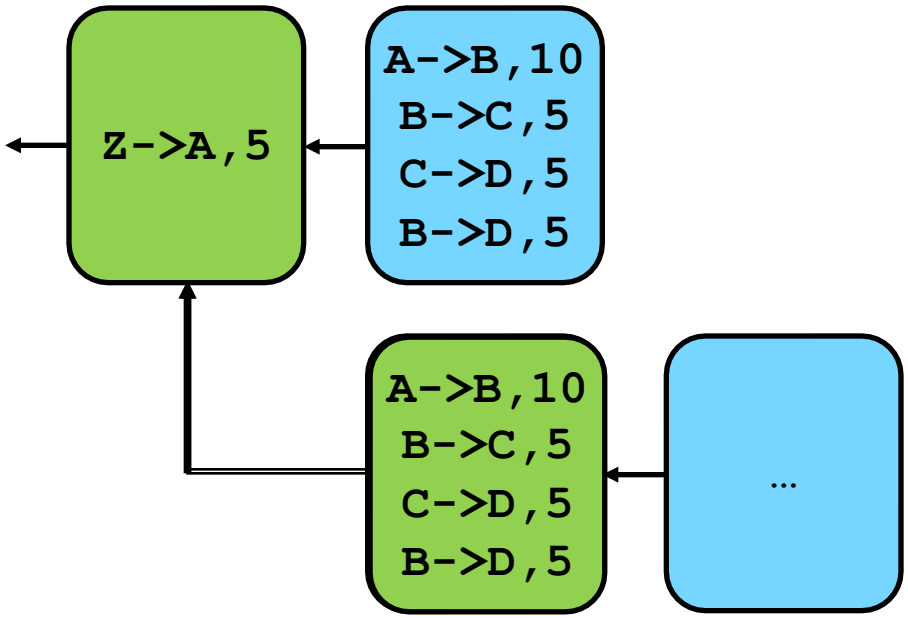
- When one block is discovered by honest nodes, pool publishes its only one private block if it is ahead of 1 block.
- Two branches of length 1 compete with each other.

Selfish Mining by Dishonest Pool : 2 branches



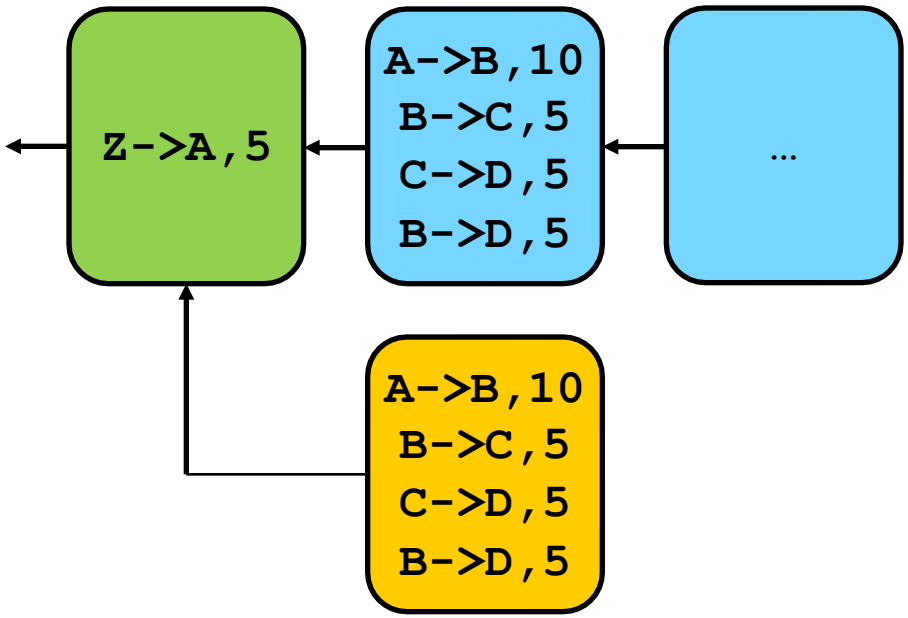
- Three possible outcomes:
  - Pool mines on private branch, discovers next block, gets bitcoins reward for 2 blocks, public branch is pruned.

Selfish Mining by Dishonest Pool : Lead by 1



- Three possible outcomes:
  - Pool mines on private branch, discovers next block, gets bitcoins reward for 2 blocks, public branch is pruned.
  - Honest miners mine on private branch, discover next block. Pool gets bitcoins reward for 1 block, public branch is pruned.

Selfish Mining by Dishonest Pool : Lead by 1



- When one block is discovered by honest nodes, pool publishes its only one private block if it is ahead of 1 block.
- Three possible outcomes:
  - Pool mines on private branch, discovers next block, gets bitcoins reward for 2 blocks, public branch is pruned.
  - Honest miners mine on private branch, discover next block. Pool gets bitcoins reward for 1 block, public branch is pruned.
  - Honest miners mine on public branch, discover next block. Pool gets 0 reward, private branch is pruned.

Continuous-time Markov Chain Model

- State = lead of the selfish pool, with zero lead in two states:
  - 0 = no branches (only a single long global public chain)
  - 0' = two branches of length 1 (one public, one private of the pool).
- Transition rate
  - 1 = total mining power = rate at which a new block is discovered by any of the minors per time unit.
  - $\alpha < 1/2$ = relative mining power of selfish mining pool = rate at which a new block is discovered by the selfish mining pool.
  - $1-\alpha$ = relative mining power of honest minors = rate at which a new block is discovered by the honest minors.
- Gain
  - R_p = Revenue of pool (per mining event).
  - R_h = Revenue of honest miners (per mining event).
  - Pool Income: $G = E[R_p]/(E[R_p] + E[R_h])$.
  - G should be α if the mining pool was honest.
  - When is $G > \alpha$?

Continuous-time Markov Chain Model

- Notations:
  - R_p = Revenue from pool
  - R_h = Revenue from honest miners
  - Gain = $E[R_p]/(E[R_p] + E[R_h])$.
- $E[R_p] = \Sigma_i E[R_p \mid X(t) = i]\pi_i^*$ where
  - $E[R_p \mid X(t) = 0] = 0$
  - $E[R_p \mid X(t) = 0'] = 2\alpha + 1.(1-\alpha)/2 + 0.(1-\alpha)/2 = (1+3\alpha)/2$
  - $E[R_p \mid X(t) = 1] = 0$
  - $E[R_p \mid X(t) = 2] = 2.(1-\alpha)$
  - $E[R_p \mid X(t) = i] = 1.(1-\alpha)$ for $i \geq 3$.
- $E[R_h] = \Sigma_i E[R_p \mid X(t) = i]\pi_i^*$ where
  - $E[R_h \mid X(t) = 0] = 1.(1-\alpha)$
  - $E[R_h \mid X(t) = 0'] = 1.(1-\alpha)/2 + 2.(1-\alpha)/2 = 3.(1-\alpha)/2$
  - $E[R_h \mid X(t) = i] = 0$ for $i \geq 1$.
- Gain = $E[R_p]/(E[R_p] + E[R_h]) = \ldots > \alpha \Leftrightarrow \alpha > 1/4$.