Proof of Stake

Arian Baloochestani

Proof of Stake

- Use **currency** as scarce recource.

One dollar = One vote

- Those with the most coins have more to lose
  - They work in the interests of the network

Proof of Stake

- Freeze a certain amount of money (**stake**) to be able to mine (mint)
- PPCoin (Peer Coin)

$$H(prevblockhash \parallel addr \parallel timeinsec) < d_0 . stake(addr)$$

- Base difficulty d_0 adjusted based on deposit $stake(addr)$
- $timeinsec$ ensures only one try every second

Proof of Stake

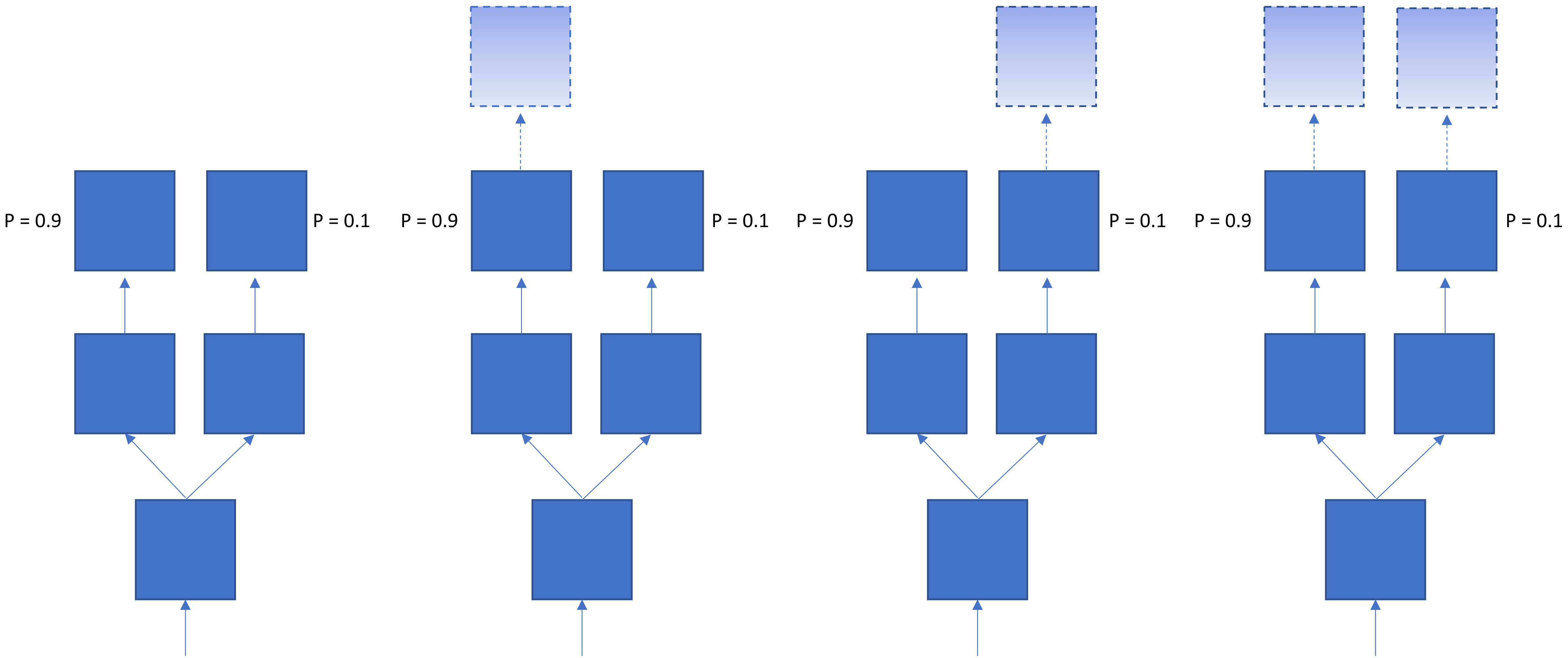
- Pros
  - **Cost efficient** (Energy, Hardware)
  - **More stakeholders = more security**
  - **More decentralized**

- Cons
  - **Economic inequality** (Rich gets richer)
  - **Nothing at stake** (Can mine on 2 different forks)
  - **Predictablity** (Will I get the next block?)
  - **Long Range attacks** (Can rewrite the complete history)

Nothing at stake

- Lose nothing by behaving badly
- Lose nothing by signing all forks
- PoW
  - Loses the computational power!
- PoS
  - Can try hashes for different last blocks in each fork per second

Nothing at stake



Reward = 0

P = 0.9

P = 0.1

Reward = 0.9

P = 0.9

P = 0.1

Reward = 0.1

P = 0.9

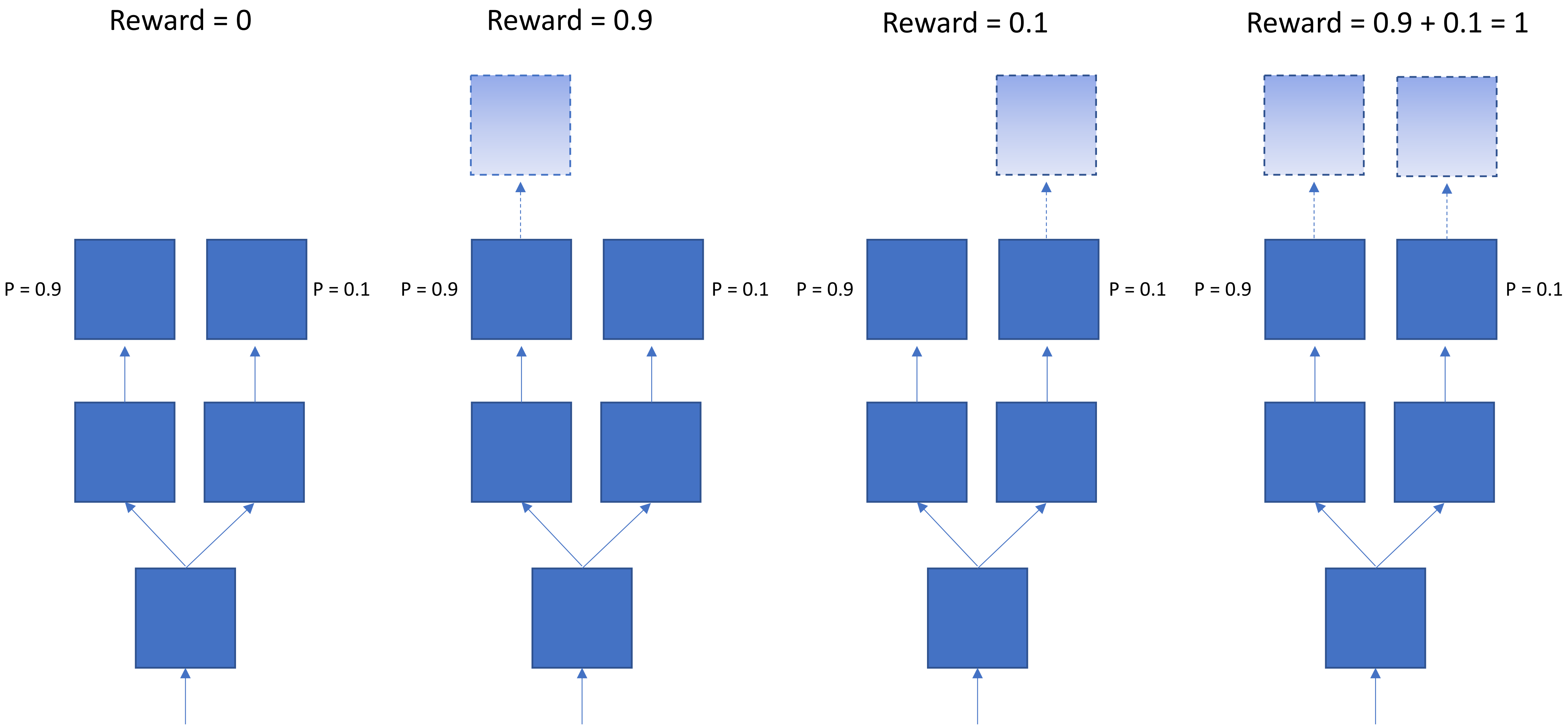
P = 0.1

Reward = 0.45 + 0.05 = 0.5

P = 0.9

P = 0.1

Nothing at stake



Reward = 0

P = 0.9

P = 0.1

Reward = 0.9

P = 0.9

P = 0.1

Reward = 0.1

P = 0.9

P = 0.1

Reward = 0.9 + 0.1 = 1

P = 0.9

P = 0.1

Nothing at stake

- Lose nothing by behaving badly
- Lose nothing by signing all forks
- Optimal strategy for miners: Mine of every chain
  - Get the reward anyway, no matter which fork wins
- Double spending with even 1% of stakes!

Nothing at stake

- Solution: **Slashing**!
- The miners stakes is freezed till a certain number of blocks
  - Deposit
- If a miner behave badly, will punished by losing the deposit
  - Punish if found a miner is mining on 2 different chains at the same time
  - Punish if found a miner is mining on a wrong chain
- What happens to the deposit?
  - Burned
  - Given to the miner who reported

Rich get richer

- Problem: The block reward directly can be used as the part of stake for the next blocks!
  - Miner with the most stakes has the most probability to be selected for the next block
  - If selected, block reward is added to its stake, and its probability increases even more!
- Solution: Coin age
  - Use time as a scarce resource
  - Coin age = The number of days the stake has been held
  - Multiply stake by coin age
  - Reset coin age when a new block is created!

Long range attacks

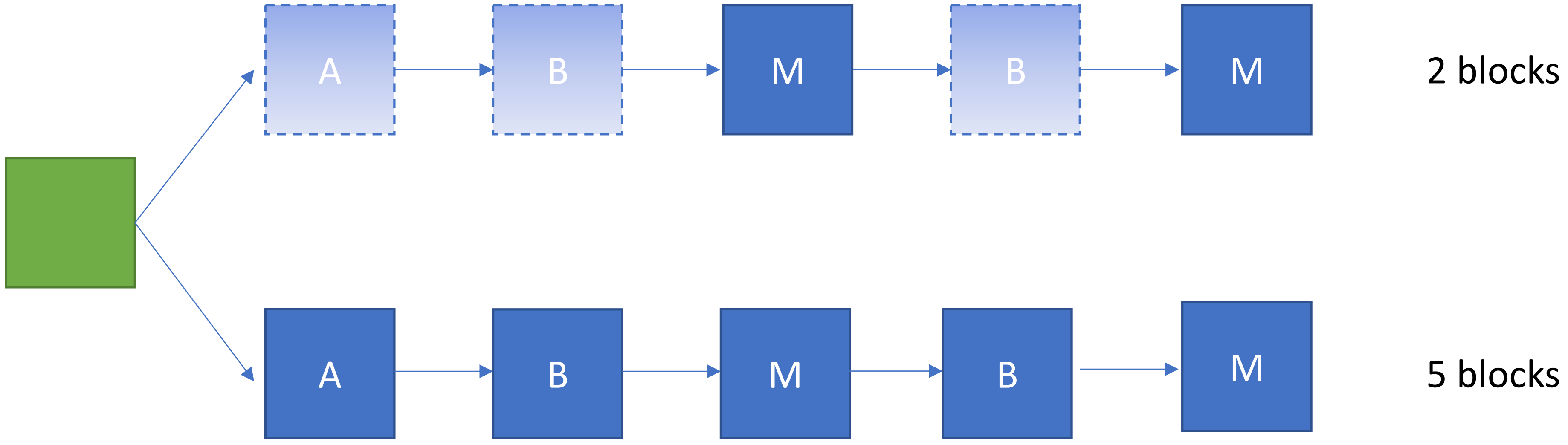
- Similar to 51% attack in Bitcoin
- A miner creates a fork on the blockchain starting from the Genesis block and overtakes the main chain
- Reasons
  - Weak subjectivity
    - Online nodes monitor the blockchain in real-time, they know the main chain
    - New nodes cannot tell which chain is the main
      - Longest chain rule
  - Nothing at stake
    - Longest chain rule is not enough

Long range attacks

- Long range attacks
  - Simple
  - Posterior Corruption
  - Stake bleeding

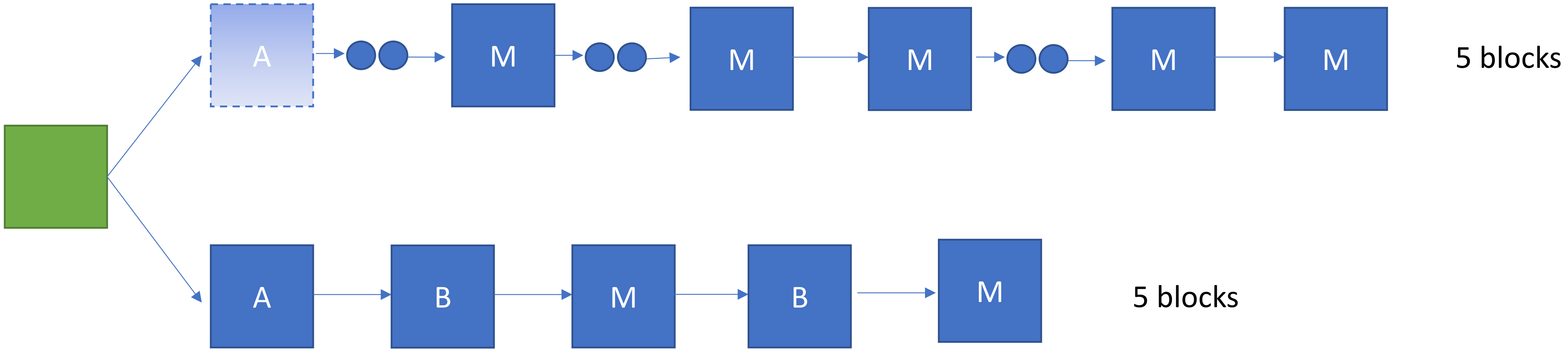
Simple long range attack

- Nodes do not check timestamps
- Attacker wants to overtake the main chain
    - can start from genesis, forge timestamps and builds a chain faster than the real chain
- Having 3 miners with same stake



Simple long range attack

- Nodes do not check timestamps
- Attacker wants to overtake the main chain
  - can start from genesis, forge timestamps and builds a chain faster than the real chain
- Having 3 miners with same stake

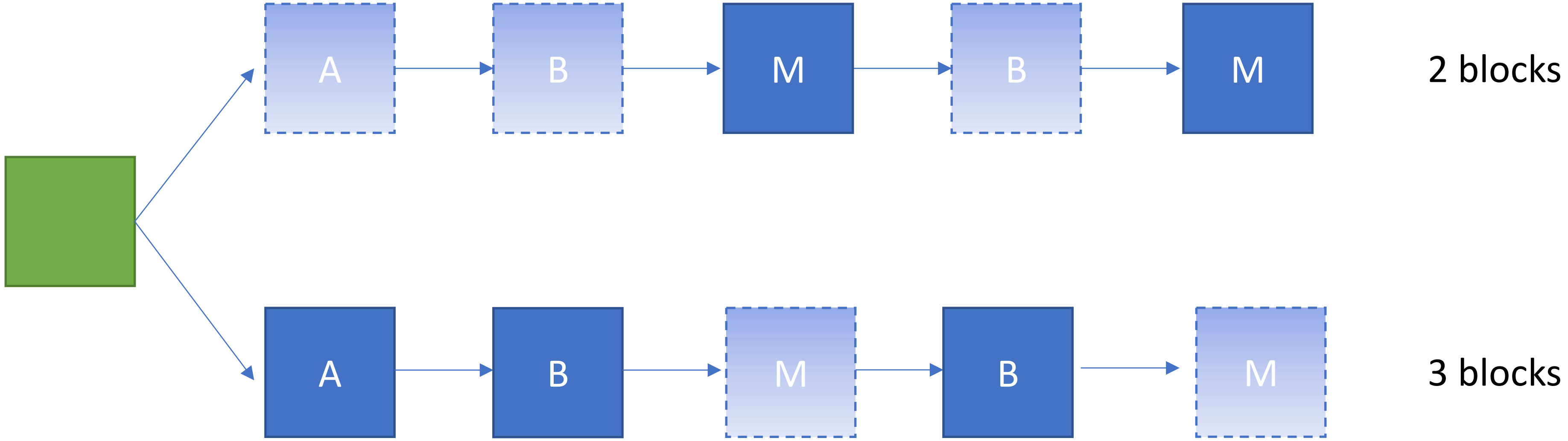


Posterior corruption long range attack

- Miners check timestamps
  - Forging timestamp is not possible
- Get access to the acounts of miners that are no longer active, but had a large stake at the beginning
  - Bribe them
  - Hack them
- If the accounts have good amount of stake, the attacker chain is built faster than main chain

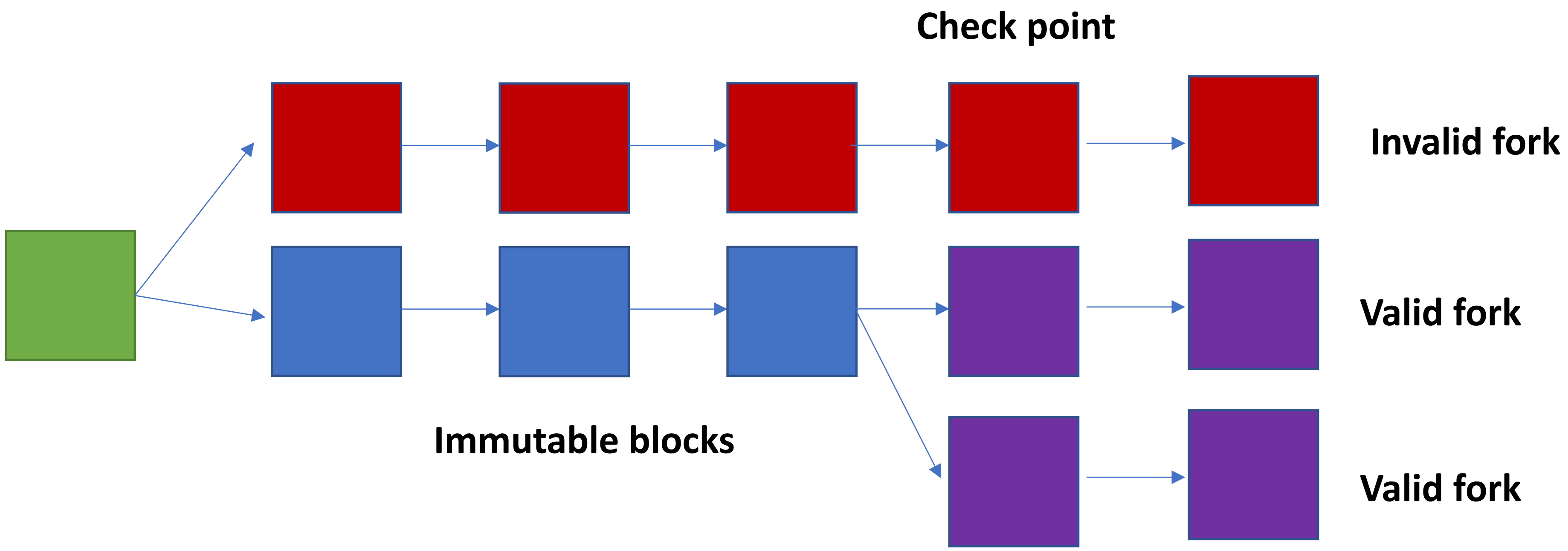
Stake bleeding long range attack

- Attacker
  - DDoS the network and other miners by any way possible
  - Increase its blocks on the private chain by increasing its stake
    - Stealing blocks from the main chain to use transaction fees
  - Very slow!



Long range attacks solutions

- Moving check points
  - Do not accept forks started before the checkpoints



Long range attacks solutions

- Moving check points
  - Do not accept forks started before the checkpoints
  - Update checkpoints frequently
    - Every 1000 blocks, every day
  - Does not solve the problem
    - Short range attacks!
  - Used for all 3 kinds of long range attacks

Long range attacks solutions

- Downtime slashing
  - Solves weak subjectivity
  - If a node remains offline for a certain amount of time, it will be punished
    - E.g. offline for more than 16 hours
  - Incentivise nodes to stay online

Long range attacks solutions

- Key-evolving cryptography
  - When miner signs the generated block, it destroys the key used for signing that block
  - Miner key evolves and changes per each generated block
  - Miners can not return to an older version of the key
  - Counters Posterior Corruption attacks

Long range attacks solutions

- Context-aware transactions
  - Include the hash of a previous block inside a transaction
  - Transactions contain a historical reference of the blockchain
    - Can not be copied in another chain that the historical reference is not there
  - Counters stake bleeding attacks