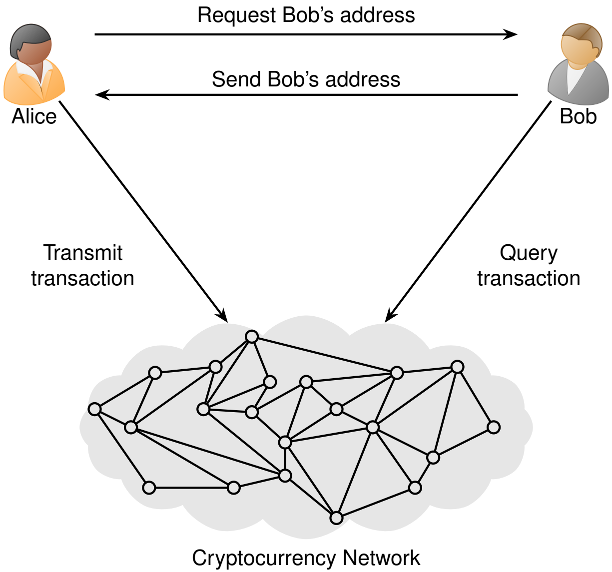
The Cost of Security in a Blockchain

Saravanan Vijayakumaran
sarva@ee.iitb.ac.in

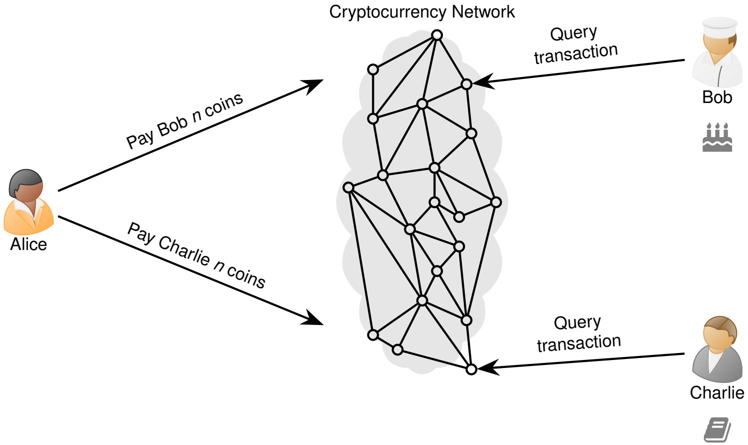
Department of Electrical Engineering
Indian Institute of Technology Bombay

September 26, 2018

Cryptocurrency Transaction Workflow



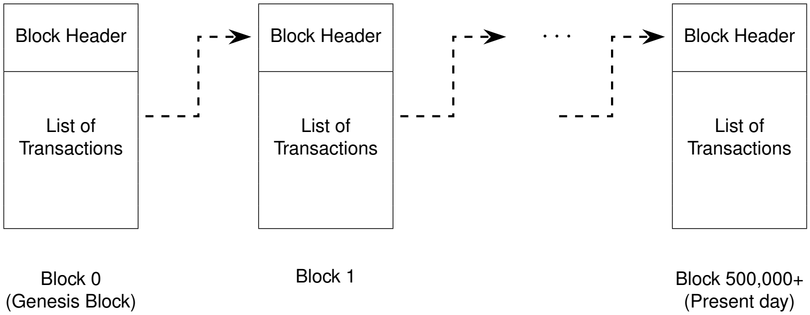
Double Spending Problem



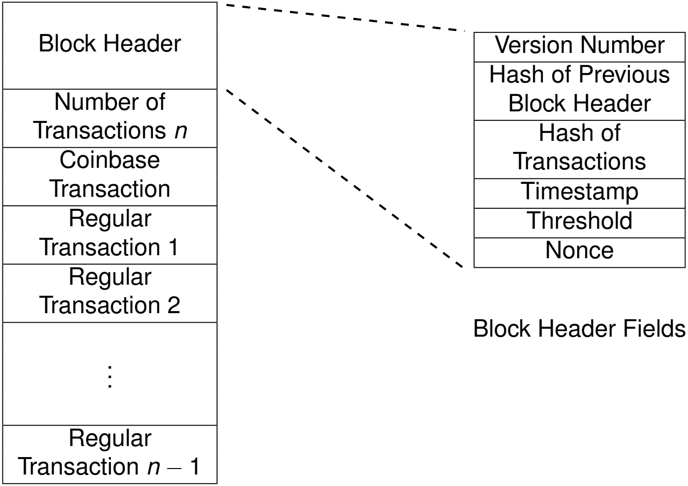
- Alice pays Bob n coins for a cake
- Alice uses the **same** n coins to pay Charlie for a book

The Bitcoin Blockchain

A public database to store all transactions which is replicated by many network nodes



Block and Header Formats



Block Header Fields

- Hash = Output of cryptographic hash function

Cryptographic Hash Functions

- Easy to compute but difficult to invert
- Collision-resistant
- Pseudorandom outputs

Input	SHA-256 Output
`bitcoin0`	`2277efd2e9051a1978682cad7a111876031f7fcdb9a2a06b5fdeee160dd8f34e`
`bitcoin1`	`dbdbac0b3072d7677fc94eebaf8eba9e81e5c3b7de6899dae12c98d6799b065a`
`bitcoin2`	`1ed7259a5243a1e9e33e45d8d2510bc0470032df964956e18b9f56fa65c96e89`
`bitcoin3`	`0c5582329503f93b4b243a986551d9e22e46ee9ba681d687078cbcbad0c7d023`
`bitcoin4`	`0a49508bf91ac4f98e6a01b575e1a3f200a5d9a03d00219aea52b15b064cdf50`
`bitcoin5`	`de6206bd52f4228ebc556c85b26e3582fa141f8839a11d2a2ca761d0f7e24ec3`
`bitcoin6`	`e1abb7b46d14bb2c3e13208ebc9790ab847f6b5265adbf154d4200b513359e22`
`bitcoin7`	`c07bed0fae2067f2ed35cc443d97aeacbaf0b59dcbd619f76c75477690b82d3b`
`bitcoin8`	`8ecc8a5ebc2a99db8e950c29242e7052ae2930cd60258176efe36750a4e33170`
`bitcoin9`	`38ab2bcafbf65eb6204162d28082ad7616f2a66f20b27696262e3842b3712d0b`

- SHA-256 = NIST approved CHF with 256-bit outputs

Cryptographic Hash Functions

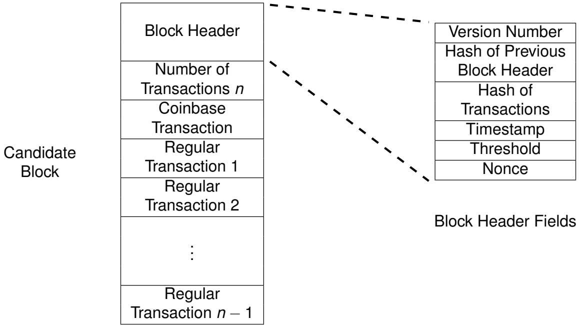
- Easy to compute but difficult to invert
- Collision-resistant
- Pseudorandom outputs

Input	SHA-256 Output
`bitcoin0`	`2277efd2e9051a1978682cad7a111876031f7fcdb9a2a06b5fdeee160dd8f34e`
`bitcoin1`	`dbdbac0b3072d7677fc94eebaf8eba9e81e5c3b7de6899dae12c98d6799b065a`
`bitcoin2`	`1ed7259a5243a1e9e33e45d8d2510bc0470032df964956e18b9f56fa65c96e89`
`bitcoin3`	`0c5582329503f93b4b243a986551d9e22e46ee9ba681d687078cbcbad0c7d023`
`bitcoin4`	`0a49508bf91ac4f98e6a01b575e1a3f200a5d9a03d00219aea52b15b064cdf50`
`bitcoin5`	`de6206bd52f4228ebc556c85b26e3582fa141f8839a11d2a2ca761d0f7e24ec3`
`bitcoin6`	`e1abb7b46d14bb2c3e13208ebc9790ab847f6b5265adbf154d4200b513359e22`
`bitcoin7`	`c07bed0fae2067f2ed35cc443d97aeacbaf0b59dcbd619f76c75477690b82d3b`
`bitcoin8`	`8ecc8a5ebc2a99db8e950c29242e7052ae2930cd60258176efe36750a4e33170`
`bitcoin9`	`38ab2bcafbf65eb6204162d28082ad7616f2a66f20b27696262e3842b3712d0b`

- SHA-256 = NIST approved CHF with 256-bit outputs
- At a billion outputs per second, 78 billion years required to calculate 2^{100} outputs

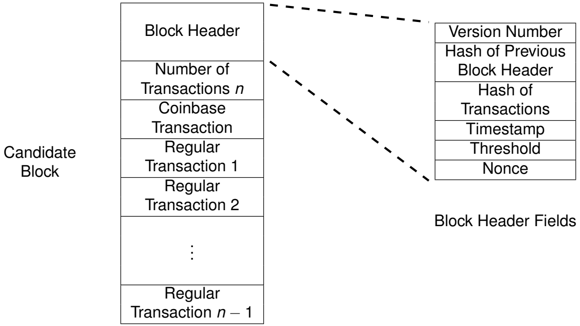
Who Adds Blocks?

- Mining = Process of adding new blocks to the blockchain
- Nodes which want to perform transactions broadcast them
- Miners collect some of these transactions into a candidate block



Who Adds Blocks?

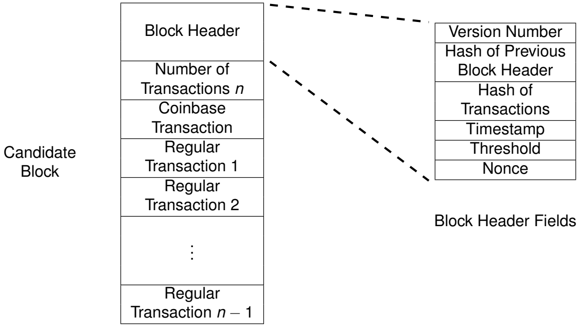
- Mining = Process of adding new blocks to the blockchain
- Nodes which want to perform transactions broadcast them
- Miners collect some of these transactions into a candidate block



- Threshold encodes a 256-bit value like 0x$\underbrace{00\cdots00}_{\text{16 times}}\underbrace{\text{FFFFF}\cdots\text{FFFFF}}_{\text{48 times}}$

Who Adds Blocks?

- Mining = Process of adding new blocks to the blockchain
- Nodes which want to perform transactions broadcast them
- Miners collect some of these transactions into a candidate block



- Threshold encodes a 256-bit value like $0x\underbrace{00\cdots00}_{\text{16 times}}\underbrace{\text{FFFFF}\cdots\text{FFFFF}}_{\text{48 times}}$
- Miner who can find Nonce such that

$$\text{SHA256}(\text{SHA256}(\underbrace{\text{Version Number} \parallel \cdots \parallel \text{Nonce}}_{\text{Candidate Block Header}})) \leq \text{Threshold}.$$

can add a new block

Mining Difficulty and Rewards

- Why is mining hard?
  - Brute-force search is the only way to find suitable nonce
  - Target area is small compared to output space of SHA256

$$\Pr\left[\text{Success in single trial}\right] \approx \frac{\text{Threshold}}{2^{256}}$$

Mining Difficulty and Rewards

- Why is mining hard?
  - Brute-force search is the only way to find suitable nonce
  - Target area is small compared to output space of SHA256

$$\Pr\left[\text{Success in single trial}\right] \approx \frac{\text{Threshold}}{2^{256}}$$

  - For 0x$\underbrace{00\cdots00}_{16\text{ times}}\underbrace{\text{FFFFF}\cdots\text{FFFFF}}_{48\text{ times}}$, success probability is $\frac{1}{2^{64}}$

Mining Difficulty and Rewards

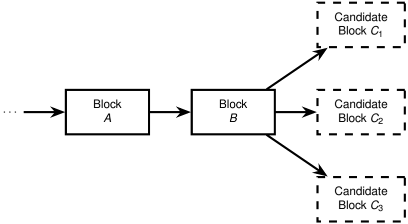
- Why is mining hard?
  - Brute-force search is the only way to find suitable nonce
  - Target area is small compared to output space of SHA256

$$\Pr\left[\text{Success in single trial}\right] \approx \frac{\text{Threshold}}{2^{256}}$$

  - For $0x\underbrace{00\cdots00}_{\text{16 times}}\underbrace{FFFFF\cdots FFFFF}_{\text{48 times}}$, success probability is $\frac{1}{2^{64}}$
- Why do mining?
  - Successful miner gets rewarded in bitcoins
  - Every block contains a **coinbase transaction** which creates 12.5 bitcoins
  - Miners also collect the transaction fees in the block

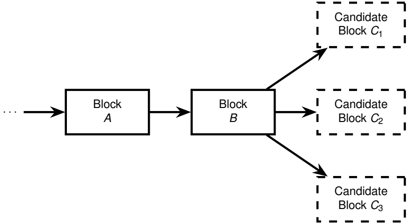
Block Addition Workflow

- Nodes broadcast transactions
- Miners accept valid transactions and reject invalid ones (solves double spending)
- Miners try extending the latest block

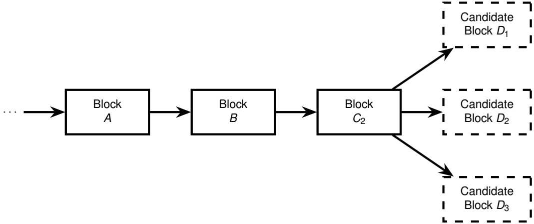


Block Addition Workflow

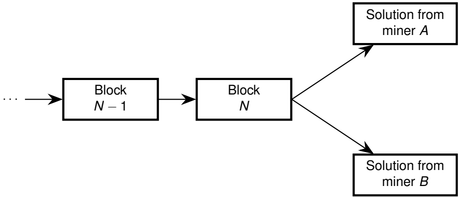
- Nodes broadcast transactions
- Miners accept valid transactions and reject invalid ones (solves double spending)
- Miners try extending the latest block



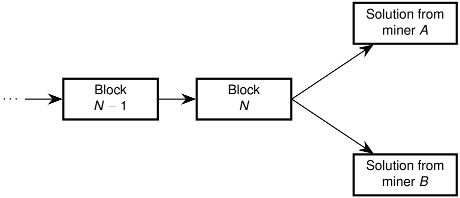
- Successful miners broadcast solutions
- Unsuccessful miners abandon their current candidate blocks and start work on new ones



What if two miners solve the puzzle at the same time?

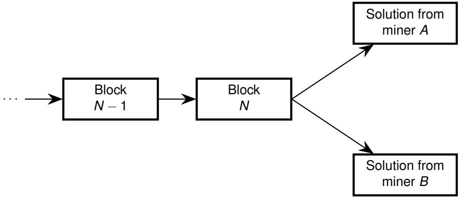


What if two miners solve the puzzle at the same time?



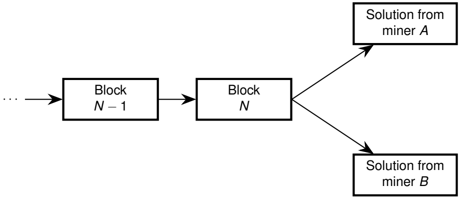
- Both miners will broadcast their solution on the network

What if two miners solve the puzzle at the same time?

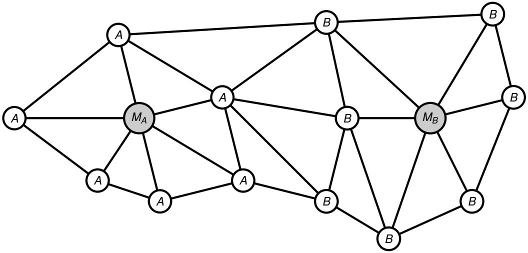


- Both miners will broadcast their solution on the network
- Nodes will accept the first solution they hear and reject others

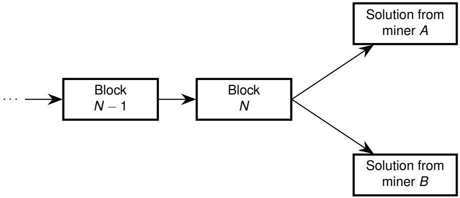
What if two miners solve the puzzle at the same time?



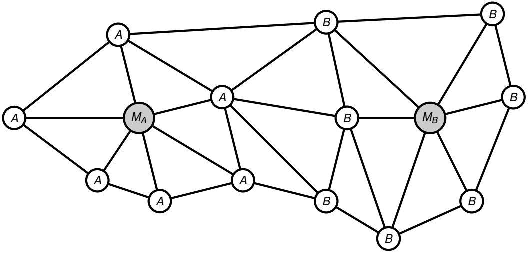
- Both miners will broadcast their solution on the network
- Nodes will accept the first solution they hear and reject others



What if two miners solve the puzzle at the same time?

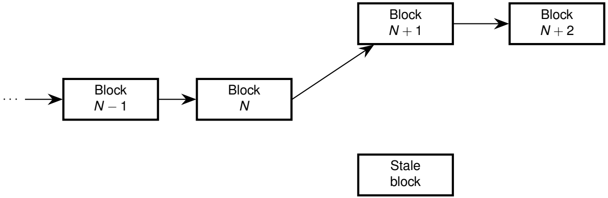


- Both miners will broadcast their solution on the network
- Nodes will accept the first solution they hear and reject others

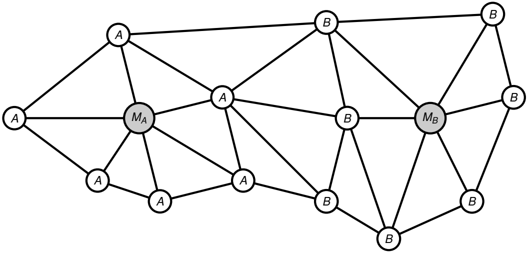


- Nodes always switch to the chain which was more difficult to produce

What if two miners solve the puzzle at the same time?

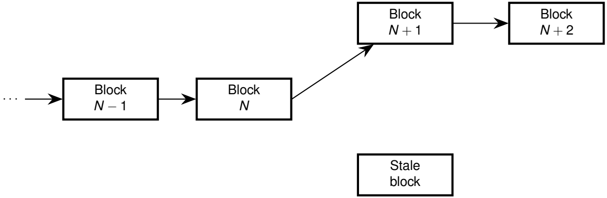


- Both miners will broadcast their solution on the network
- Nodes will accept the first solution they hear and reject others

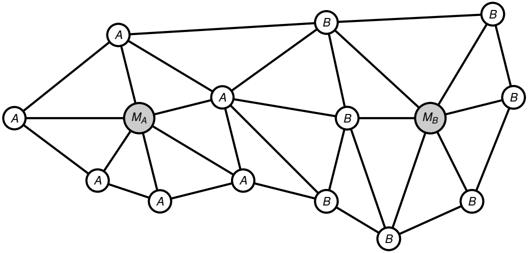


- Nodes always switch to the chain which was more difficult to produce

What if two miners solve the puzzle at the same time?



- Both miners will broadcast their solution on the network
- Nodes will accept the first solution they hear and reject others



- Nodes always switch to the chain which was more difficult to produce
- Eventually the network will converge and achieve consensus

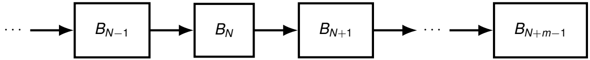
Tamper Resistance

- Suppose Alice wants to modify block B_N

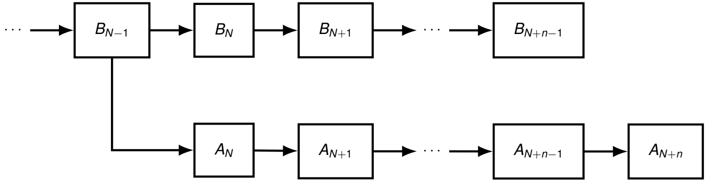
$$\cdots \longrightarrow \boxed{B_{N-1}} \longrightarrow \boxed{B_N} \longrightarrow \boxed{B_{N+1}} \longrightarrow \cdots \longrightarrow \boxed{B_{N+m-1}}$$

Tamper Resistance

- Suppose Alice wants to modify block B_N

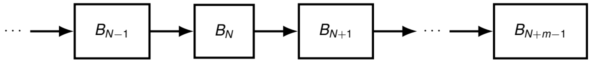


- Alice works on A_N branch; other miners work on B_N branch

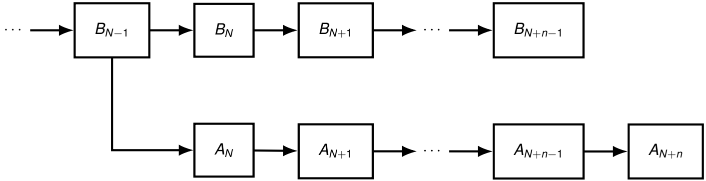


Tamper Resistance

- Suppose Alice wants to modify block B_N



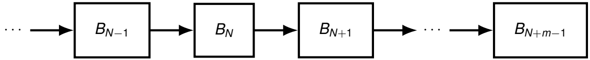
- Alice works on A_N branch; other miners work on B_N branch



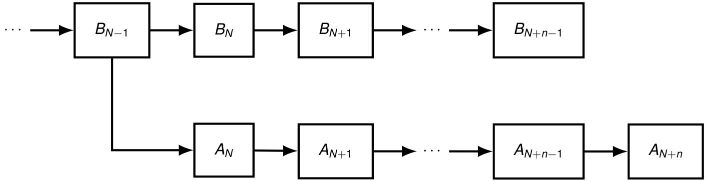
- She needs to mine blocks faster than the rest of the miners

Tamper Resistance

- Suppose Alice wants to modify block B_N



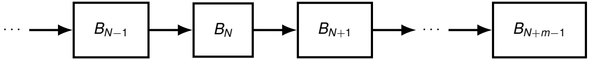
- Alice works on A_N branch; other miners work on B_N branch



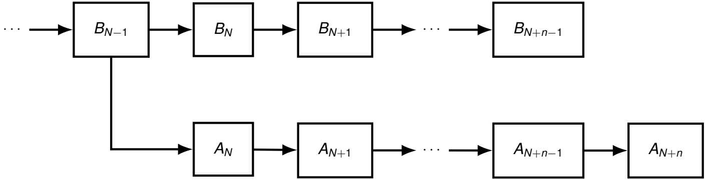
- She needs to mine blocks faster than the rest of the miners
- Possible if she controls 50% or more of network hashrate

Tamper Resistance

- Suppose Alice wants to modify block B_N



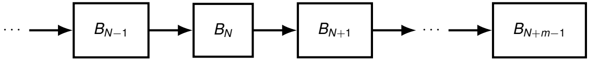
- Alice works on A_N branch; other miners work on B_N branch



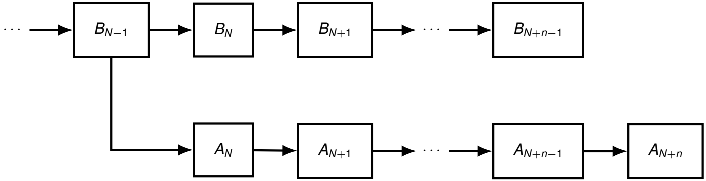
- She needs to mine blocks faster than the rest of the miners
- Possible if she controls 50% or more of network hashrate
- Current network hashrate $\approx$ 50 EH/s = 50×10^{18} H/s

Tamper Resistance

- Suppose Alice wants to modify block B_N



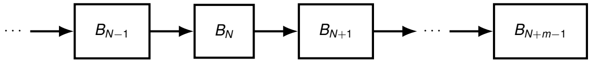
- Alice works on A_N branch; other miners work on B_N branch



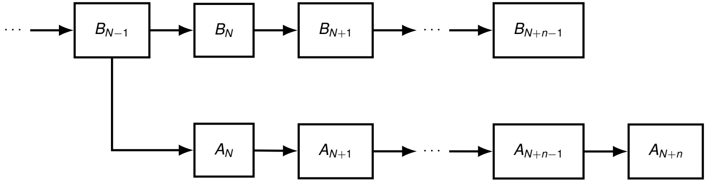
- She needs to mine blocks faster than the rest of the miners
- Possible if she controls 50% or more of network hashrate
- Current network hashrate $\approx$ 50 EH/s = 50×10^{18} H/s
- One mining unit costing \$450 gives 14.5 TH/s

Tamper Resistance

- Suppose Alice wants to modify block B_N



- Alice works on A_N branch; other miners work on B_N branch



- She needs to mine blocks faster than the rest of the miners
- Possible if she controls 50% or more of network hashrate
- Current network hashrate $\approx$ 50 EH/s = 50×10^{18} H/s
- One mining unit costing \$450 gives 14.5 TH/s
- Controlling 50% of hashrate = Controlling 775 million USD worth of hardware

Challenges for Enterprise Blockchains

- Proof-of-work consensus is not suitable
- Proof-of-authority is an alternative but insecure
  - A valid block is one with a certain number of approvers
  - Collusion between approvers can rewrite history

Challenges for Enterprise Blockchains

- Proof-of-work consensus is not suitable
- Proof-of-authority is an alternative but insecure
  - A valid block is one with a certain number of approvers
  - Collusion between approvers can rewrite history
- Possible solution = Checkpointing on public blockchains

Challenges for Enterprise Blockchains

- Proof-of-work consensus is not suitable
- Proof-of-authority is an alternative but insecure
  - A valid block is one with a certain number of approvers
  - Collusion between approvers can rewrite history
- Possible solution = Checkpointing on public blockchains

Thanks for your attention