CSE446: Blockchain & Cryptocurrencies

Lecture – 18: Blockchain Security & Advanced Topics

Inspiring Excellence

Agenda

- Blockchain Security
- Advanced Topics

Blockchain Security

- Transaction censoring attack
- 51% attack
- Double-spending attack
- Selfish mining attack (Block withholding attack)
- Nothing-at-stack attack
- Sybil attack
- DDoS attack

Transaction censoring attack

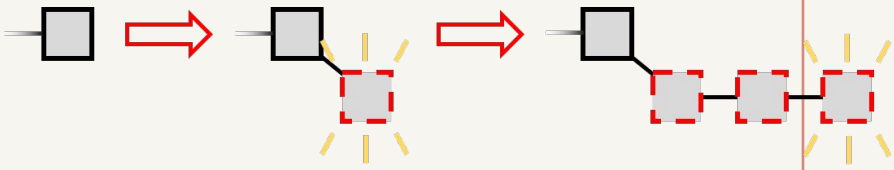
- Blocking (censoring) a transaction from a certain address (people)
- Malicious validating (full) nodes:
  - As long as there are majority of honest nodes (>50%), the transactions will be propagated
  - Mind you, a malicious node cannot affect the blockchain in this way
- Malicious mining nodes:
  - If malicious mining nodes censor transactions, they would still be included in a block mined by an honest node

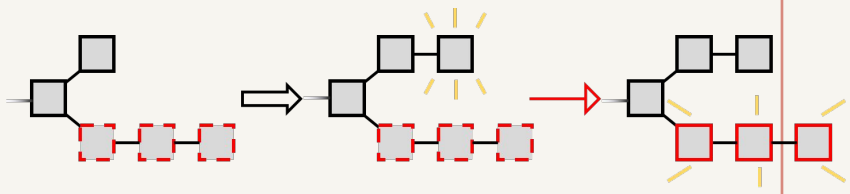
51% attack

- A group of malicious nodes can collude to launch the infamous 51% attack
- It happens in PoW-based blockchains, if a single miner's hashing power accounts for more than 50% of the total hashing power of the entire blockchain
- In PoS blockchain, 51% attack may also occur if the number of coins owned by a single miner is more than 50% of the total blockchain
- Controlling a majority (51%) can cause a deliberate "fork" in the blockchain
  - A fork is where the attacker causes previously confirmed blocks to be invalidated by forking below them and re-converging on an alternate chain
  - With sufficient power, attackers can generate blocks at a faster rate than honest miners
  - This will result in the invalid chain to be longer than the shorter chain, ultimately becoming the main chain

Selfish mining (block withholding) attack

- An attack to PoW blockchain
- The attacker (selfish miner) privately generates valid blocks and extends their own chains secretly, forming a secret branch
- The selfish miner continues to extend her secret branch until the public chain is one step behind
- Then she publishes her secret chain
- Since the secret chain is longer, the other parties consider it the main chain, so now everyone is following the selfish miner's blocks
- The blocks generated by the other miners are ignored
- The selfish miner can reap rewards for multiple blocks together

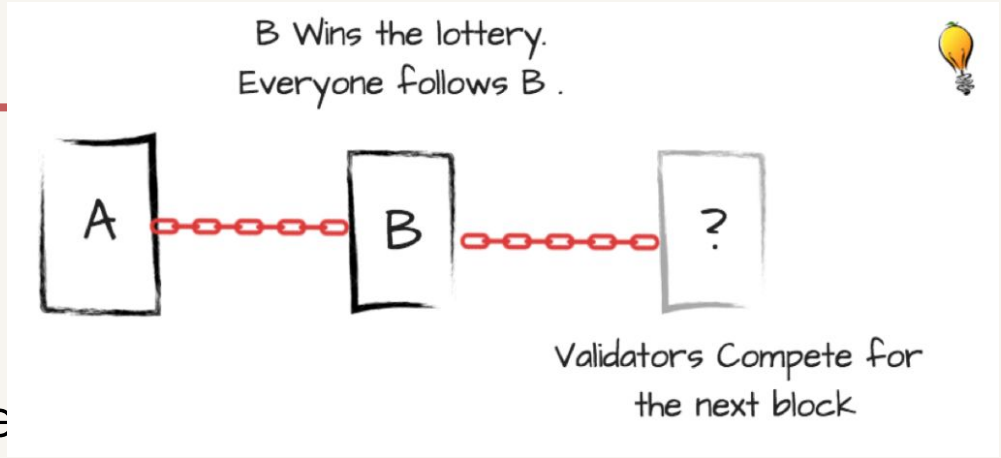


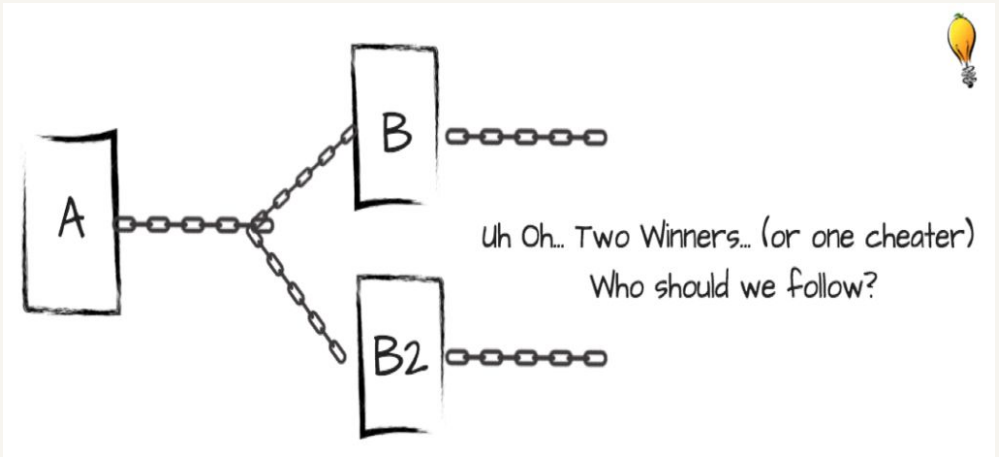


https://decentralizedthoughts.github.io/2020-02-26-selfish-mining/

Nothing-at-stake attack

- In PoS, participants compete in a lottery to win the right to propose the next block
- The winner's block is either accepted or rejected – and the process continues with the chain being extended on each "accepted" block
- Things are tricky when there is "Fork" for:
  - There's a malicious attack – an attempt to reverse a transaction
  - Two winners are chosen

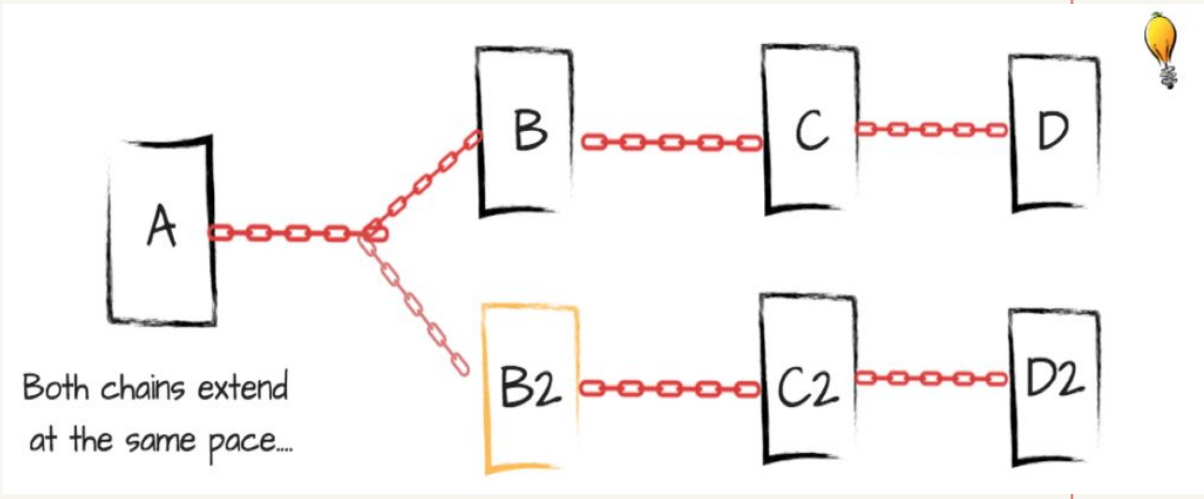




https://www.mangoresearch.co/casper-nothing-at-stake-problem/

Nothing-at-stake attack

- An attacker might attempt to add its newly created block in all forked branches to increase their probability to add their block as the valid block
- Since it does not cost anything for a validator in a PoS algorithm to add blocks in multiple parallel branches, the attacker is motivated to do so
- Applying a penalty for such misbehaviour could effectively tackle this problem



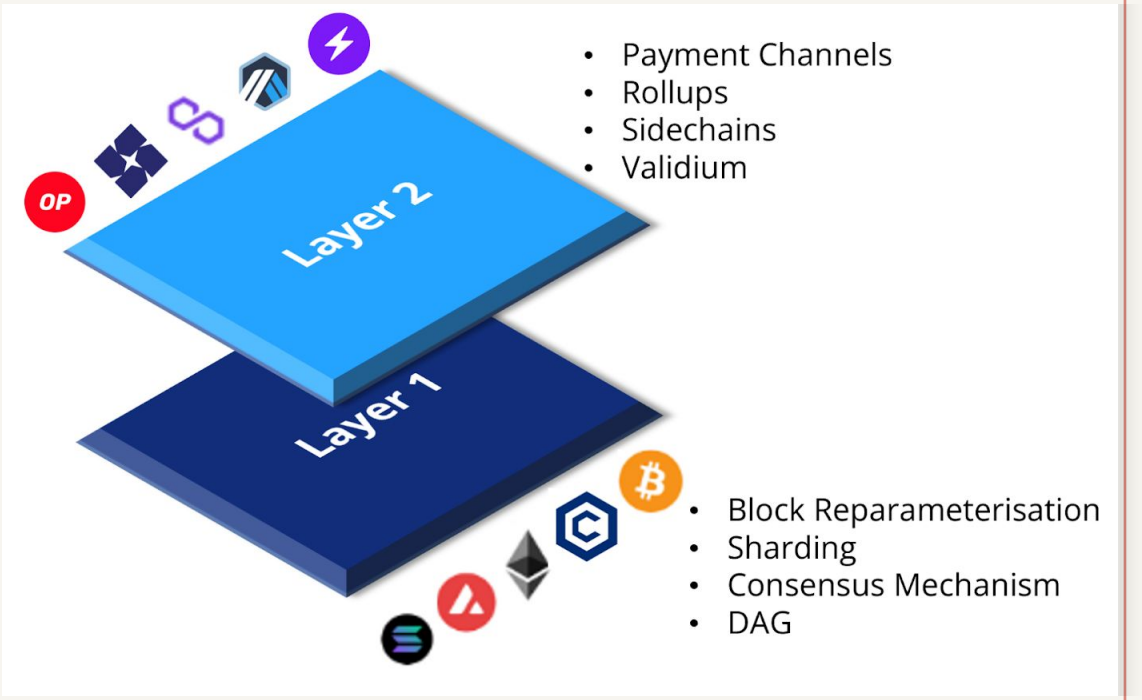
https://www.mangoresearch.co/casper-nothing-at-stake-problem/

Advanced concepts

- Three major advanced concepts to address the scalability and privacy issues of blockchain
  - Layer 2 solution
  - Sharding
  - ZKP (Zero-knowledge Proof)

Layer 2 solution

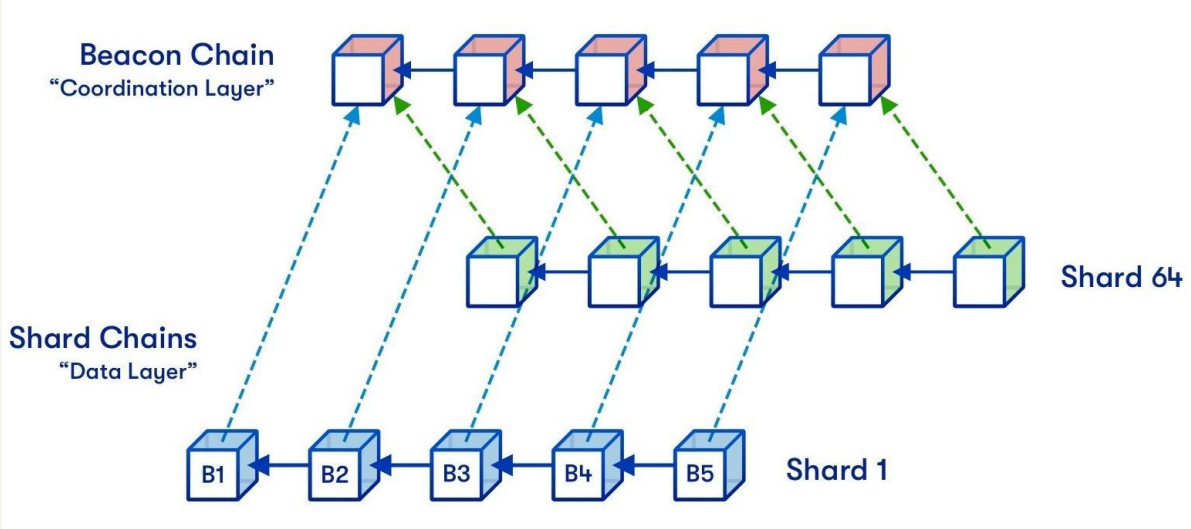
- Layer-1 refers to the main blockchain
- Layer-2, however, is an overlaying network that sits on top of the main blockchain
- Lightning Network is the Layer-2 solution for Bitcoin
- Plasma, Polygon, Optimism, and Arbitrum are just a few of the Layer-2 networks built on Ethereum



https://lh4.googleusercontent.com/B1uC_R-1QjLjiUyluH8AsNvIypLA08KJhh4xKimpCIxzJscitYNgrsixZmcnhAj0Umq_bL7yghOzr9nyRQjAsL66uQjxGG8YQoMvNKRmVz1-g0nWxkh3OOl1BaIAHgnmreXsLAmcRe7m1R_C6Q

Sharding

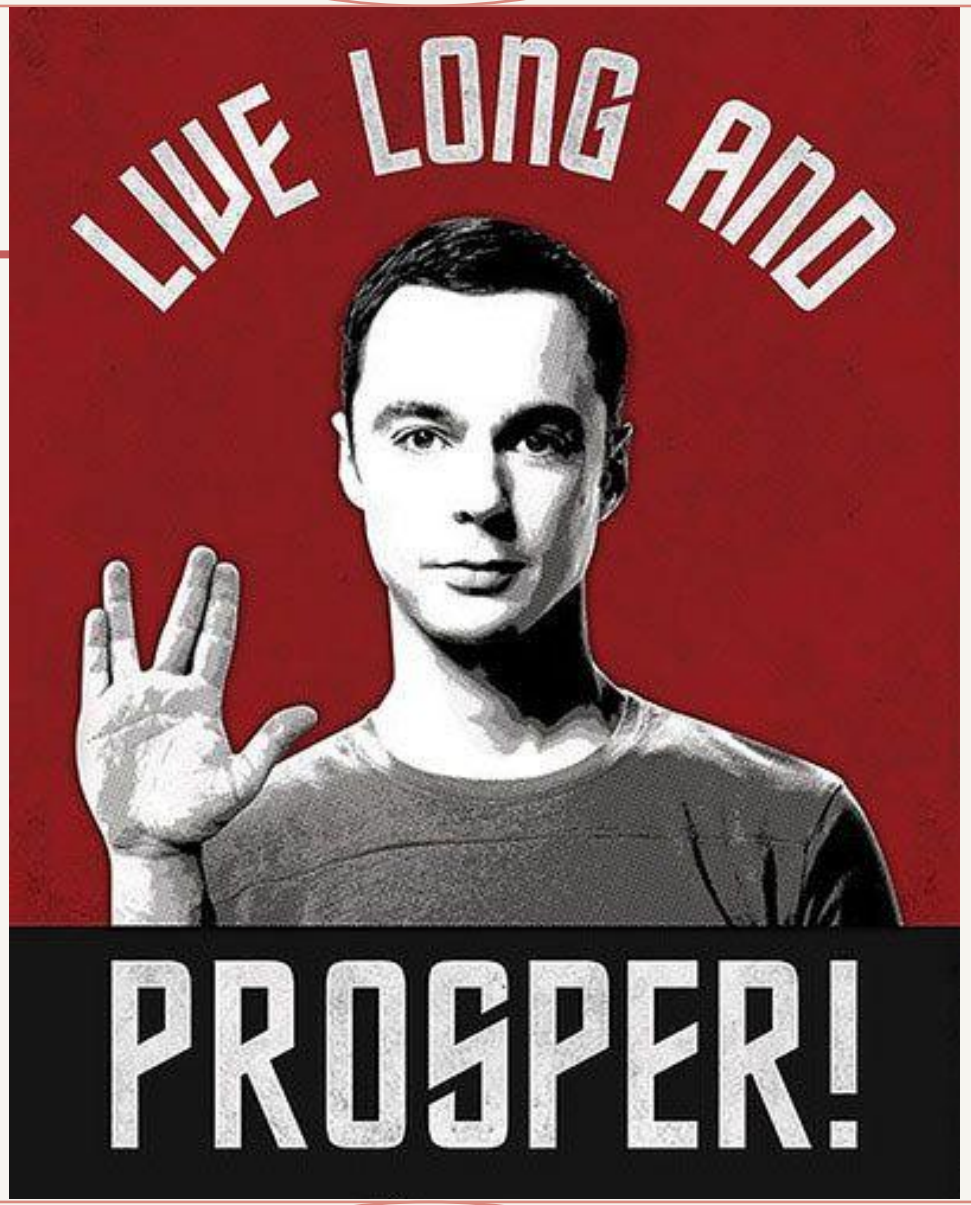
- Sharding is a method of database partitioning that is utilised by blockchain organisations to increase scalability
- This enables them to execute a greater number of transactions per second and store data across multiple nodes in a sustainable way



https://vitalik.ca/images/sharding-files/beacon_chain.jpg

ZKP (Zero-knowledge Proof) in blockchain

- ZKP is a method by which one party can interact with another party and provides proof of knowledge without unveiling their confidential data
  - Say there are two millionaire and they would like to determine who is richer without revealing their total assets
  - Logging in to an online system without providing passwords
- ZKP facilitates this by using cryptographic mechanisms
- In blockchain, ZKP facilitates private transactions and others
  - Nobody in the blockchain knows who is the sender and who is the receiver
- Example: ZCash


LIVE LONG AND
PROSPER!