CSE 3550/5000: Blockchain Technology

Lecture 5

Bitcoin - Part III

Ghada Almashaqbeh

UConn - Spring 2026

Outline

- Ledger security notion.
- Security threats in Bitcoin.

Ledger Security

Security Properties (informally)

- A ledger L is secure if it satisfies the following properties:
  - **Safety:** For any two time rounds *t1* and *t2* such that *t1* ≤ *t2*, and any two honest parties P1 and P2, the confirmed state of L maintained by P1 at *t1* is a prefix of the confirmed state of L maintained by party P2 at time *t2* with overwhelming probability.
  - **Liveness:** If a valid transaction tx is broadcast at time round *t*, then with overwhelming probability it will be recorded on L at time at most *t+u*, where *u* is the liveness parameter.
- As such, a secure blockchain grows over time and records only valid transactions and blocks in an immutable way, i.e., confirmed blocks and transactions cannot be altered, with a consistent view of the confirmed chain among the miners.
- The ledger protocol is parameterized by predicates to verify transaction and block validity

Bitcoin Security Issues

Security Issues

- We will explore the following:
  - Double spending.
  - Sybil attacks.
  - 51% attack.
  - Eclipse attack.
  - Goldfinger attacks.
  - Denial of service attacks.
  - Anonymity and transaction linkability.

Double Spending

- Spend the same coins more than once.
  - All what costs the owner to do so is to produce a new signature.
- Handled by logging all transactions on the blockchain.
  - Miners check whether a transaction input has been already spent, and if so, they reject the double spending one.
- Network propagation delay may allow race condition, and hence double spending, between transactions.
  - Also manipulating the transaction fee may allow that.
  - how?
- To address this issue, usually it is advised not to act (like sending a product or stock shares) until the transaction is confirmed.
  - In Bitcoin this happens when the block containing this transaction is buried under 6 blocks.
  - Advised to wait even longer for large-value transactions.

Sybil Attacks

- An attacker creates a large number of fake identities to control the majority of the network.
  - Other examples; manipulating reputation-based systems (e.g., restaurants ratings on yelp, or Amazon reviews).
- Bitcoin thwarts Sybil attacks through the use of proof-of-work as we discussed previously.
  - So creating new identities is expensive as computation power is needed to mine a new block.
  - Recall that mining a new block is an implicit vote on the previous block ⇒ no computing power to mine means no voting power..

51% Attack

- Blockchains are append-only logs.
- If a blockchain is mutable, then several security issues would arise.
  - E.g., double spending will be easy. Alice pays Bob and the transaction is confirmed, then Alice can go back and modify the transaction like deleting it or direct the output to herself.
- If Alice control >= 51% of the mining power, then she create a longer branch, which the miners will adopt, and succeed in double spending even if the blockchain is immutable?!
  - Due to owning >= 51% of the network's mining power, she will be able to produce blocks at a faster rate than the rest of the miners in the network.
- 51% attack is believed to be very hard.
  - Thus, a basic security assumption in blockchains is that the majority of the mining power is honest.

Tendency Toward Centralization

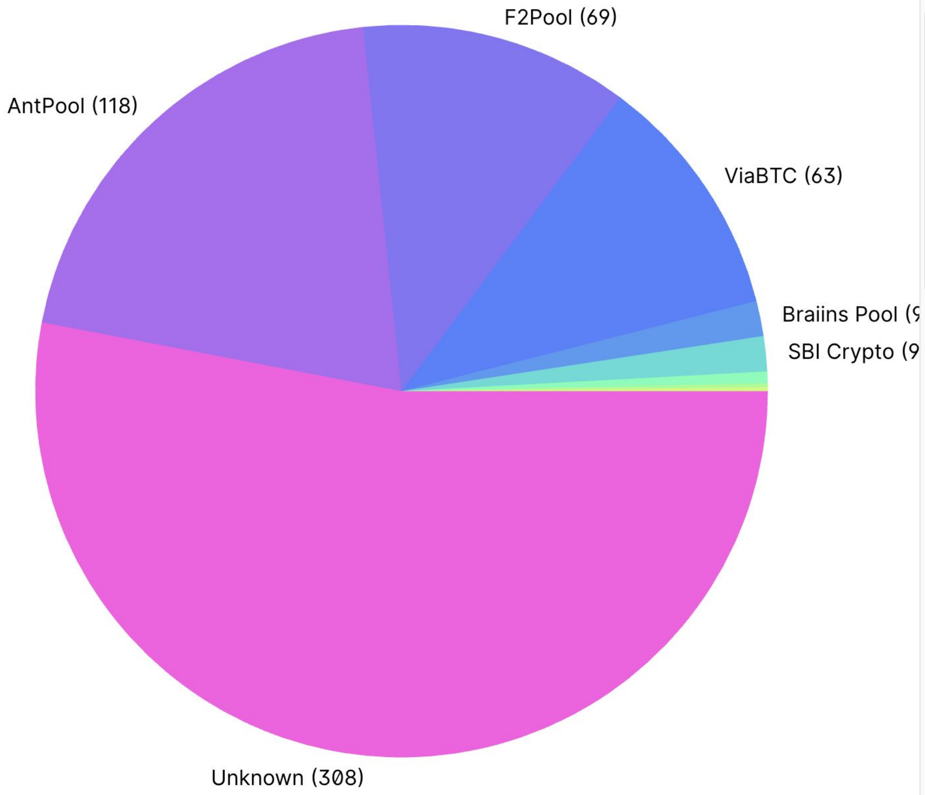
- Bitcoin (and other cryptocurrencies) has tendency toward centralization.
- Reasons:
  - Even though mining is open to anyone it is not the case now, you need expensive powerful mining hardware to be able to compete with the powerful miners out there.
  - In early 2009 miners were using CPUs, then GPUs, and now it is ASIC (application specific integrated circuits).
- The mining algorithm (proof-of-work in case of Bitcoin) is outsourceable, i.e. you can ask someone else to do the work for you.
- This encouraged the concept of ***mining pools*** where a set of miners get together under the control of a single party called the pool manager.
- This is a general problem in all cryptocurrencies that uses outsourceable mining algorithm.

Mining Pools I

- Mostly centralized, each pool is under the control of one manager.
- The manager does the following:
  - keep a registration directory of all active miners,
  - build a block candidate for each round, distribute this block among all miners in the pool each of which will work on a different nonce range in parallel to solve the PoW puzzle,
  - receive mining shares from the miners to track the amount of work done by each one.
  - The mining reward goes to the manager address after which it is distributed among all miners based on the contributed shares with some fee goes to the manager.
- There are different types of pools with different policies of distributing the mining rewards.
- In all centralized mining pools miners must trust the manager.

Mining Pools II

- ~85% of Bitcoin network mining power is under the control of 3 mining pools!
- Thus, 51% attack is way easier to be performed now if pool managers collude with each other.
    - What prevents them from doing that?
- Source: https://blockchain.info/pools



Eclipse Attack

- Monopolize all connections to and from specific node(s).
- Thus, an attacker can control the view that this node has about the network and the blockchain.
  - Control which transactions/blocks/information (like control messages) this node receives from the network.
  - Control which transactions/blocks/information sent by this node will be received by the rest of the network.
- Can this attack be useful to perform double spending for example? how?

Goldfinger Attack

- Destroy a system in favor of another system or group of entities.
- For example, a group of miners may collude to take a competing cryptocurrency down in order to keep Bitcoin as the leading currency.
    - Happened in practice, it is believed that an altcoin called CoiledCoin was destroyed by Eligius (a Bitcoin mining pool).
- This highlights the difficulty of modeling incentive compatibility in open-access distributed systems.
    - It is not only internal, it should account for external influencing factor.

Denial of Service Attacks

- Interrupting the service and making it unavailable to legitimate users.
- This may happen in blockchain-based systems, examples:
    - Miners may ignore all transactions coming from a specific client, or all blocks mined by a specific miner, or protocol updates announced by the system developers.
- What is needed to make the aforementioned attacks work?
    - Eclipse attack.
    - Majority of the miners agree to perform this attack (i.e. controlling more than 50% of the network mining power).
    - Or flooding the network/particular parties with messages.
- In general, secure system design practices need to be followed to mitigate DoS just like any other distributed system.
    - E.g., maintain high connectivity with peers, rate limiting, etc.

Anonymity, Privacy and Transaction Linkability

- Is Bitcoin anonymous?
  - Believed to be, users use random-looking public keys/addresses.
  - To preserve anonymity, create new key pair for each new transaction and send the change to a new address each time.
- It is not; transactions are linkable!
  - You can track user activity and cluster keys together, then link them back to the real user ID.
- Is Bitcoin private?
  - No, everything is logged publicly (in the clear) on the blockchain.
  - Anyone can retrieve any transaction and see its full content.
- We will study anonymity/privacy at a greater depth towards the end of the semester.