CSE5095-010: Blockchain Technology

Lecture 5

Ghada Almashaqbeh
UConn - Fall 2020

Outline

- More about Bitcoin:
  - Scalability.
    - Segregated witness.
    - Lightning networks.
  - Security.
    - Security properties,
    - Security threats.

Bitcoin Scalability

Transaction Throughput

- Bitcoin block size is limited to 1 MB and the block generation rate is around 10 minutes.
  - The average transaction size is 500 bytes.
- This limits the number of transactions per second the Bitcoin network can handle, which is 7 tx/sec.
- Comparing this to centralized payments services: Paypal handles around 500 tx/sec, Visa handles around 4000 tx/sec.
- Such low throughput drives clients to increase the transaction fees in order for their transactions to be processed faster.
- Micropayments, or payments in pennies, are not practical in this setup.
- Some solutions:
  - Segregated witness.
  - Payment channels and networks.

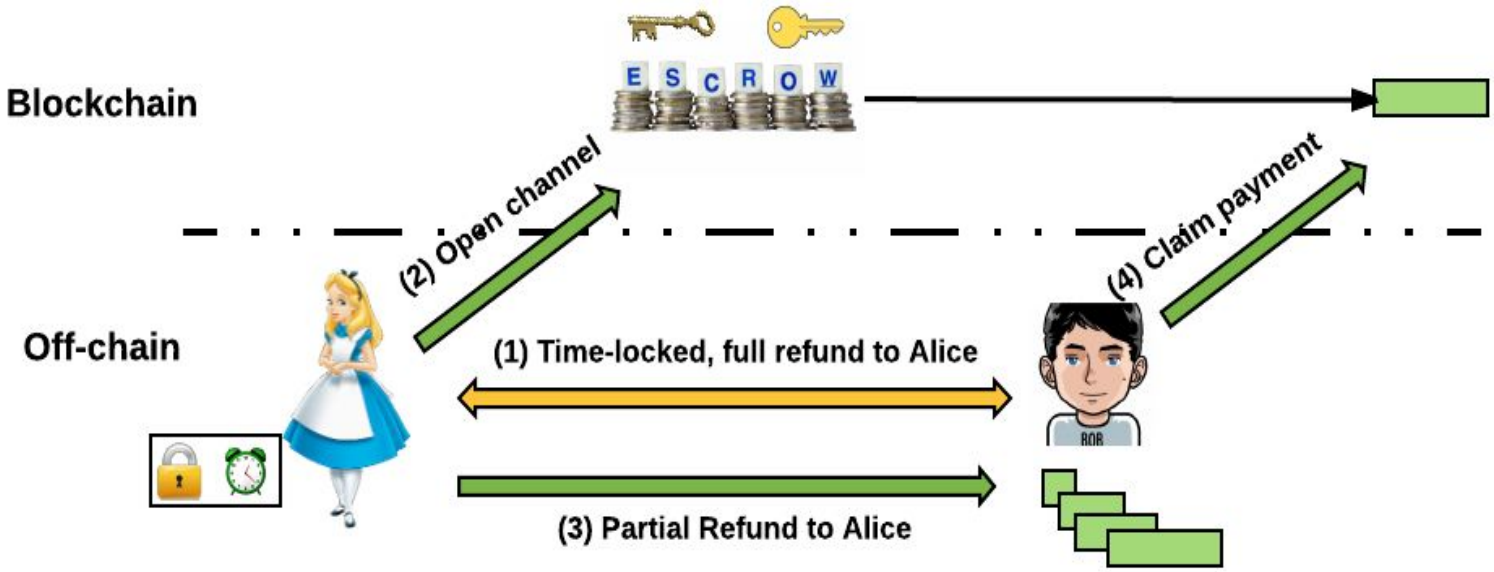
Segregated Witness (SegWit)

- Soft fork that was implemented in 2017.
- It separates the signature, i.e., witness, from the transaction body.
  - Only the transaction body is counted in the block size.
- This means that the signature is no longer part of the transaction ID.
  - Recall that a transaction ID is the hash of the transaction.
- In theory, this will increase a block size to around 4 MB, and hence, increase the transaction throughput.
  - Is this true? Check the blockinfo website!

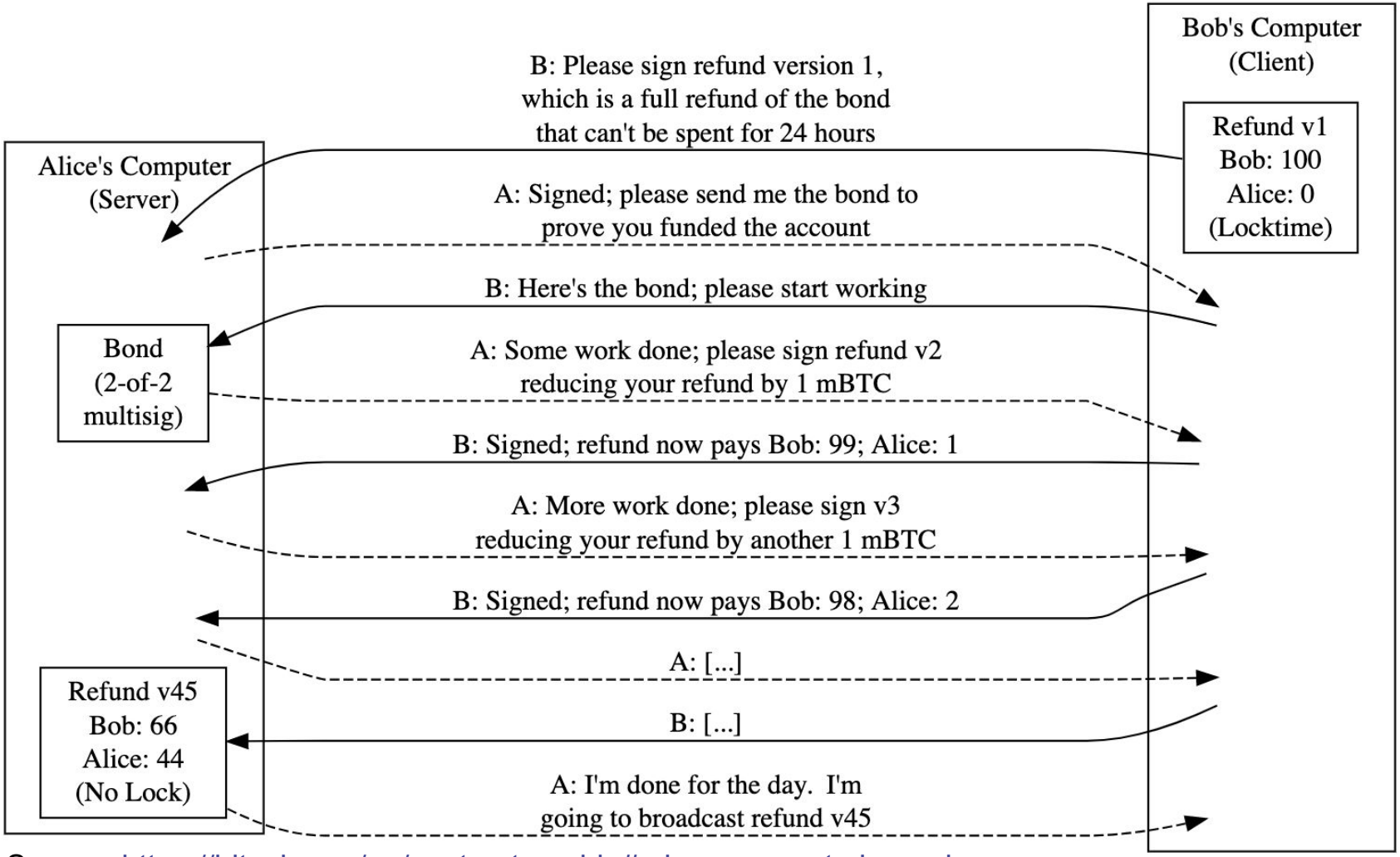
Payment Channels

- A payment channel is a contract between two parties locking a shared fund with an amount that is adjusted over time.
- It is a way of processing transactions locally, or off-chain, to reduce the number of on-chain transactions (or transactions that are logged on the blockchain).
- A channel consists of two transactions:
  - Channel opening: a multi-sig transaction locking funds in an escrow.
  - Channel closing: a refund transaction expressing the latest state of the shared fund (how it is divided between the payer and the payee).

A Payment Channel Pictorially I



A Payment Channel Pictorially II



Source: https://bitcoin.org/en/contracts-guide#micropayment-channel

Payment Networks

- Payment channels allow only two parties to exchange payments.
- Payment networks allow any two parties that share a payment path to exchange payments.
  - A payment path is a set of contiguous payments channels connecting the payer and the payee.
  - Parties in between are called payment hubs, they may charge a fee for relaying payments.
- Main example is lightning networks.
- Main disadvantage: may drive the system towards centralization.
  - Only wealthy parties may afford being hubs as it needs locking funds for each established channel.

Bitcoin Security

Security Definition

- There is no specific security notion for a cryptocurrency system.
  - Some informal definitions refer to stability of the system, meaning that a cryptocurrency will continue to behave as outlined in its design as it grows and novel attacks are attempted.
- Several works in the literature studied the security of the blockchain and the consensus protocol.
  - Defined rigorous security notions in terms of security properties that if satisfied the consensus protocol is considered secure.
  - Proved formally the security of Nakamoto's consensus protocol.

Security Properties I

- Informally, the blockchain (and its consensus protocol) is considered secure if it achieves the following properties:
  - **Consistency:** At any point in time, honest miners hold copies of the blockchain that have a common prefix and may differ only in the last y blocks, where y is a block confirmation parameter. A block then is confirmed once it is buried under y blocks on the blockchain.
  - **Future-self consistency:** At any two points in time, t1 and t2, the blockchain maintained by an honest party may differ only in the last y blocks. Consistency and future-self consistency properties achieve blockchain persistence or immutability.

Security Properties II

- **Fairness:** Miners collect mining rewards in proportion to the resources they expend in the mining process.
- **Correctness or Chain Quality:** All the blocks within the longest branch in the blockchain are valid.
- **Growth or Liveness:** As long as the system is functional, new valid blocks will be added to the blockchain.

Security Issues

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

Double Spending

- Spend the same currency 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 can check whether a transaction has been already spent or not.
- Network propagation delay may allow race condition between transactions.
  - Also manipulating the transaction fee.
- 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.

But … Transaction Processing Delay

- When a transaction is considered confirmed on the blockchain?
  - In bitcoin, this happens when buried under 6 blocks, which is around 60 min.
- Hence, a wise merchant must wait one hour to make sure that his payments are confirmed before handing the customer the purchased item.
- But assume that you are buying a cup of coffee! Are you willing to wait one hour to get it?
- Miners usually give higher priority to transactions with larger fees to be included in the next block they are working on. So, it may take your transaction longer than 1 hour to be confirmed.

Sybil Attacks

- An attack usually takes place when an attacker creates a large number of fake identities to control the majority of the network.
- Usually has the target of destroying reputation-based systems (think of restaurants ratings on yelp and Amazon reviews).
- Bitcoin thwarts this threat through the proof-of-work performed by the miners.
    - So creating new identities is expensive as computation power is needed to mine a new block, and hence, vote in the system on the previous block.

51% Attack

- Blockchains are append-only logs.
- If a blockchain is mutable, then several security issues.
  - E.g., double spending will be easy. Alice pays Bob and the transaction is confirmed, then Alice go and fork the blockchain and work on a new branch that spends the currency she paid to Bob back to herself.
- Miners then adopt the longer branch and Alice's plan work?!
  - It works in case that Alice owns at least 51% of the network computing power to be able to produce blocks at a faster rate than the rest of the miners in the system.
- Believed to be very hard to achieve since Alice needs lots of money to buy the needed computing power.

Tendency Toward Centralization

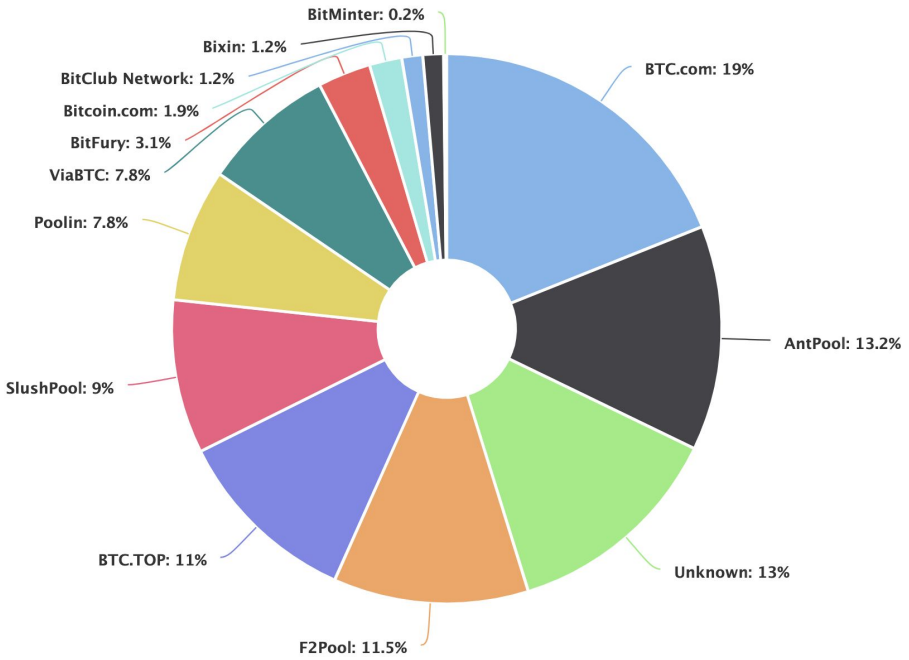
- Bitcoin (and other cryptocurrencies) have tendency toward centralization.
- Reasons:
  - Even though mining is open to anyone it is not the case now, you need to purchase expensive mining hardware to be able to compete with the powerful miners out there.
  - In early 2009 miners were using CPUs, then 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 in the mining networks 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,
  - 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.
- Different types of pools with different policies of distributing the mining rewards.
- In all centralized mining pools miners must trust the manager not to run away with the mining reward.

Mining Pools II

- ~ 95% of Bitcoin network mining power is under the control of 10 mining pools.
- Thus, 51% attack is way easier to be performed now, all what it needs is subset of those managers to collude with each other.
- https://blockchain.info/pools



Eclipse Attack

- Monopolize all connections to and from specific node(s).
- Thus, the attacker is controlling the view of this node about the network and the blockchain.
- Hear specific transactions and control what this node can inform the network about.
- Can you figure out how this attack could be useful to perform double spending for example?

Goldfinger Attack

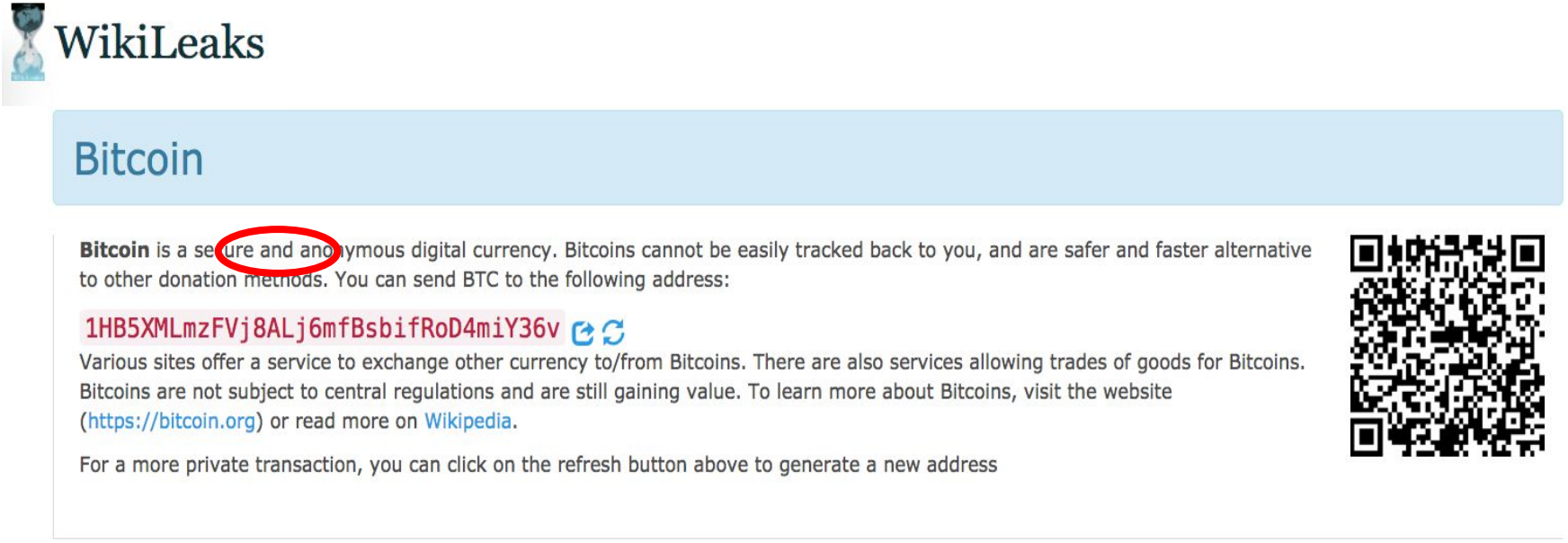
- Destroy a system in favor for another system or group of entities.
- For example, a group of miners may collude to take a competing currency down in order to keep Bitcoin as the leading currency.
  - Happened in practice, CoiledCoin was an altcoin that was destroyed by a significant attack from Eligius, a Bitcoin mining pool.
- This highlights the difficulty of modeling incentive compatibility in open access, distributed systems.

Denial of Service Attack

- Miners may ignore all transactions that are coming from a specific client/node.
- Or miners may ignore all mined blocks coming from a specific miner.
- Or miners may ignore protocol updates announced by the system developers.
- What is needed to make the aforementioned attacks work?
  - Eclipse attack.
  - Or majority of the miners agree to perform this attack (i.e. controlling more than 50% of the network computing power).

Is Bitcoin Anonymous?

- Believed to be, users are known by their public keys.
  - To protect privacy create new key pair for each new transaction.
  - Send the change to a new address each time.



Source (accessed 11/23/2017): https://shop.wikileaks.org/donate

No, it is not … Transaction are Linkable!

- Proved to be pseudo-anonymous:
- The blockchain is public, track the flow of transactions.
- Cluster Bitcoin addresses into entities, link them to identities and/or Bitcoin addresses posted by their owners on forums, etc., [Reid et al. 2014]
- Link this flow to users' IPs [Koshy et al. 2014].