CSE 5095-007: Blockchain Technology

Lecture 5
Bitcoin - Part III

Ghada Almashaqbeh
UConn - Fall 2021

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.

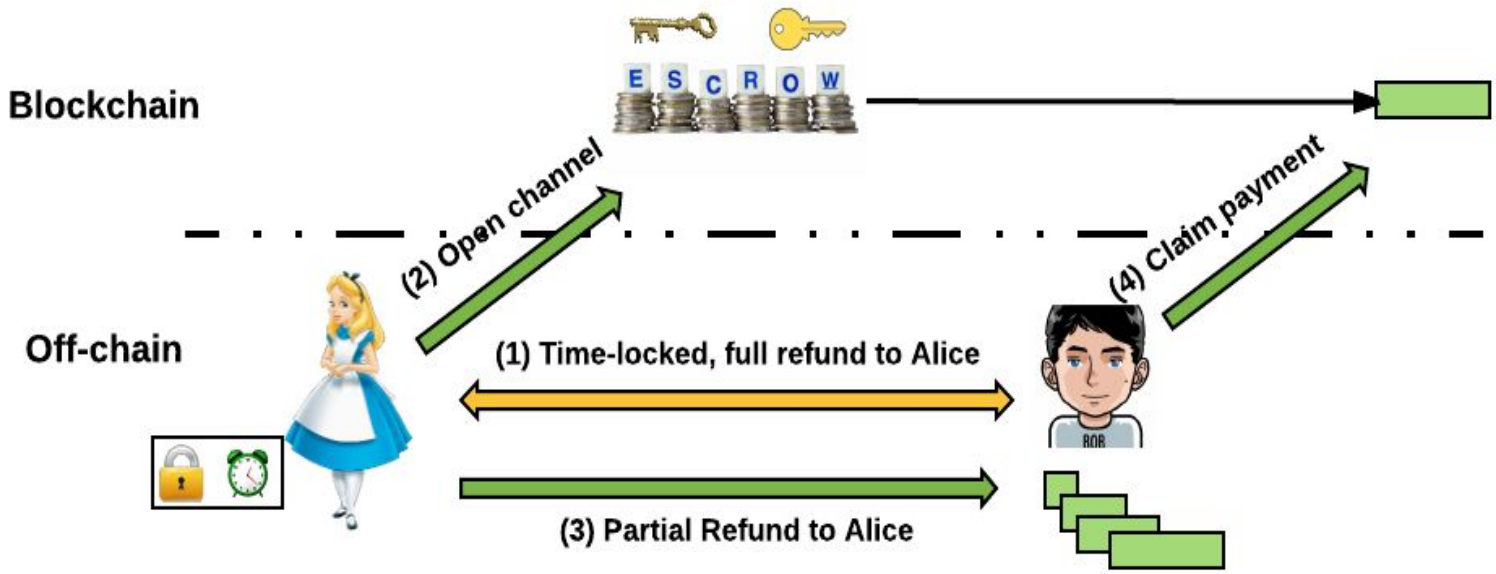
Segregated Witness (SegWit)

- 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!

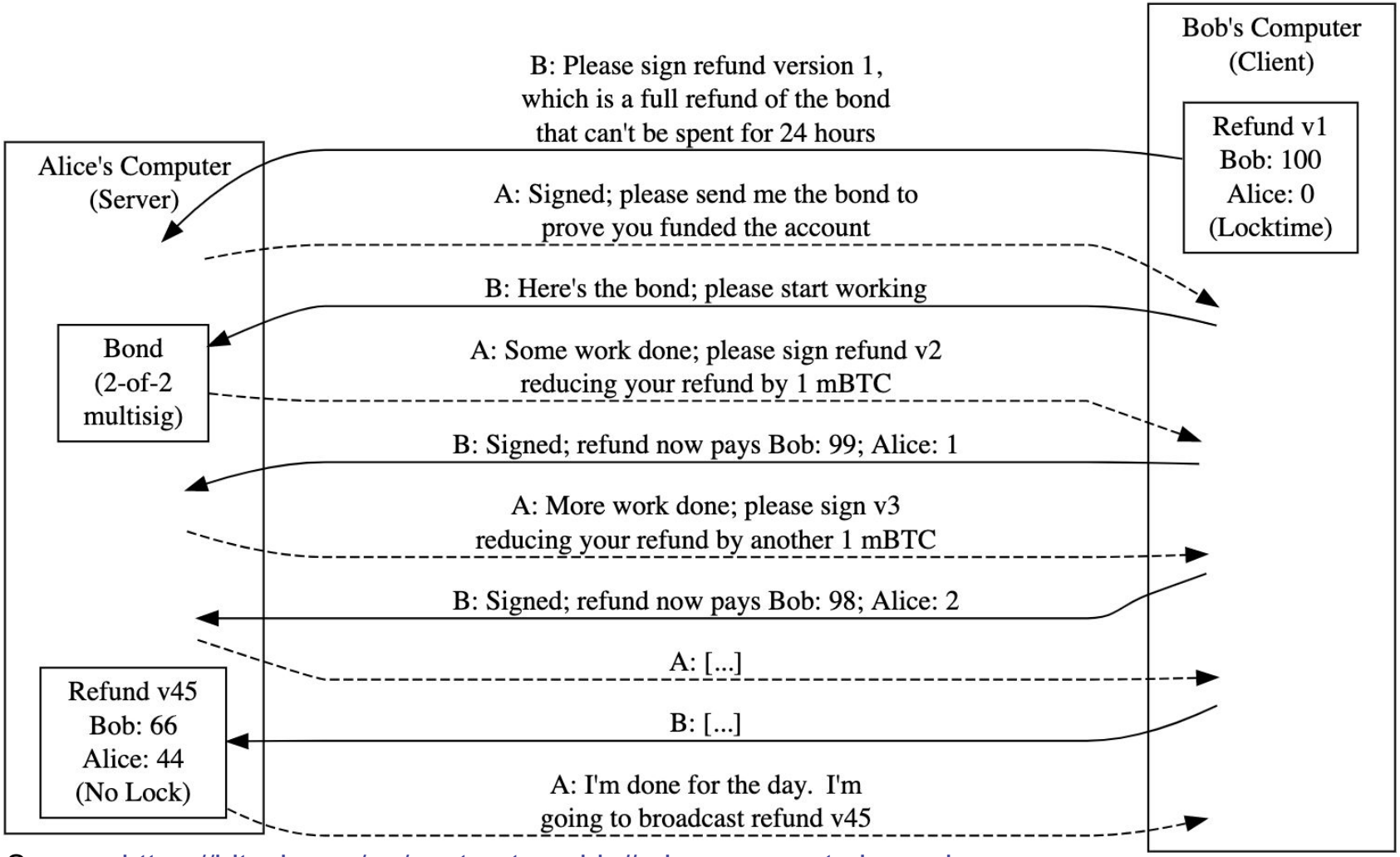
Payment Channels

- 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 payment 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 [Poon et al., 2014].
- 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 despite its growth and any attempts of novel attacks.
- Several works in the literature studied the security of the blockchain and the consensus protocol.
  - Defined rigorous security notions in terms of security properties, which if satisfied a consensus protocol is considered secure.
  - Proved formally the security of Nakamoto's consensus protocol and others.

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.
    - I.e., a block 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

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

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, and hence double spending, between transactions.
  - Also manipulating the transaction fee may allow that.
- 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.

Sybil Attacks

- An attacker creates a large number of fake identities to control the majority of the network.
  - Other examples; destroying reputation-based systems (think of restaurants ratings on yelp and Amazon reviews).
- Bitcoin thwarts miners' sybil attacks through the use of proof-of-work.
  - 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.

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.
- But if Alice creates a longer branch, which the miners will adopt, then she will succeed even if the blockchain is immutable?!
  - It works in case that Alice owns at least 51% of the network's mining power to be able to produce blocks at a faster rate than the rest of the miners in the system.
- 51% attack is believed to be very hard.
  - Thus, a basic security assumption is that the majority of the mining power is honest.

But, Tendency Toward Centralization

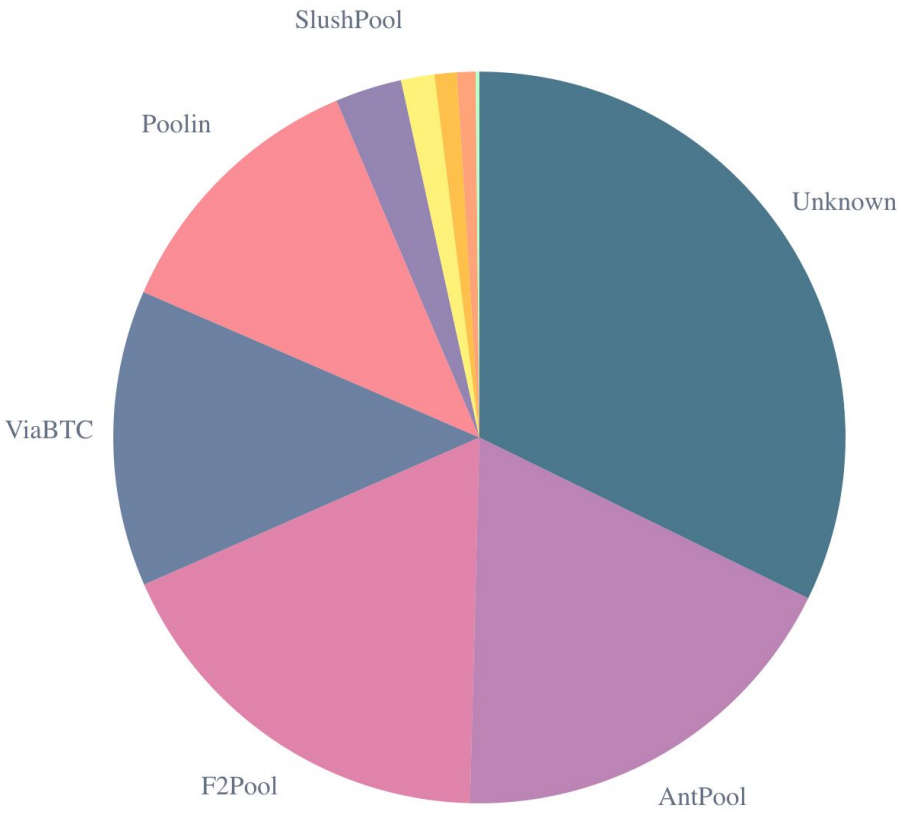
- Bitcoin (and other cryptocurrencies) has tendency toward centralization.
- Reasons:
  - Even though mining is open to anyone it is not the case now, you need to purchase expensive mining hardware to be able to compete with the powerful miners out there.
  - In early 2009 miners were using CPUs, then 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*** 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.

Mining Pools II

- ~>90% of Bitcoin network mining power is under the control of 5 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.
- What prevents them?
- Source: https://blockchain.info/pools



Eclipse Attack

- Monopolize all connections to and from specific node(s).
- Thus, an attacker controls the view of this node about the network and the blockchain.
  - Control what transactions and blocks this node receives from the network.
  - Control what transactions/blocks/information sent by this node will be received by the rest of the network.
- Can 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, it is believed that an altcoin called CoiledCoin 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 Attacks I

- Interrupting the service and make it unavailable to legitimate users.
- This may happen in blockchain-based systems, examples:
  - Miners may ignore all transactions coming from a specific client/node, 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.
  - Or majority of the miners agree to perform this attack (i.e. controlling more than 50% of the network computing power).
- In general, secure system design practices need to be followed to mitigate DoS just like any other distributed system.

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.

WikiLeaks

Bitcoin

Bitcoin is a secure and anonymous digital currency. Bitcoins cannot be easily tracked back to you, and are safer and faster alternative to other donation methods. You can send BTC to the following address:

36EEHh9ME3kU7AZ3rUxBCyKR5FhR3RbqVo

Various sites offer a service to exchange other currency to/from Bitcoins. There are also services allowing trades of goods for Bitcoins. Bitcoins are not subject to central regulations and are still gaining value. To learn more about Bitcoins, visit the website (https://bitcoin.org) or read more on Wikipedia.

For a more private transaction, you can click on the refresh button above to generate a random **Segwit (BIP-49)** address.

Please **do not** use old (1HB5X...) donation address. (message signed with old address here)

Source: https://shop.wikileaks.org/donate

No, it is not … Transaction are Linkable!

- Proved to be pseudo-anonymous:
- The blockchain is public, one can 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].

References

[Poon et al., 2014] Poon, Joseph, and Thaddeus Dryja. "The bitcoin lightning network: Scalable off-chain instant payments." Technical Report (draft) (2015).

[Reid et al. 2014] Reid, Fergal, and Martin Harrigan. "An analysis of anonymity in the bitcoin system." In Security and privacy in social networks, pp. 197-223. Springer New York, 2013.

[Koshy et al. 2014] Koshy, Philip, Diana Koshy, and Patrick McDaniel. "An analysis of anonymity in bitcoin using p2p network traffic." In International Conference on Financial Cryptography and Data Security, pp. 469-485. Springer, Berlin, Heidelberg, 2014.