Bitcoin and Cryptocurrency Technologies
Lecture 10: Other Cryptocurrencies

Yuri Zhykin

May 30, 2021

Problems and Solutions

- As of 2021, there is more than 4000 cryptocurrencies, most of which have no useful application.
- Various cryptocurrencies claim to “solve” one or several problems of Bitcoin protocol, such as:
  - weak/inflexible scripting system,
  - mining centralization,
  - energy consumption,
  - **transaction privacy**.
- Bitcoin, unlike most other cryptocurrency systems, does not have a **central governing body**.

Scripting System 1/3

- One of the first ideas of the “next generation” cryptocurrencies: make the transaction validation language Turing-complete to allow arbitrary “smart contracts”.
- A **smart contract** is a **self-executing** contract with the terms of the agreement between the parties specified as code.

Scripting System 2/3

- Bitcoin Script is a **simple stack-based Turing-incomplete** language by design.
- Bitcoin's approach:
  - simple language is easier to analyze for incorrect behavior
  - Turing-incompleteness prevents infinite loops and undefined behavior
  - most "smart contracts" are simple enough to be expressed in Bitcoin Script
  - "smart contracts" that cannot be expressed in Bitcoin Script, can/should be implemented as second-layer protocols

Scripting System 3/3

- Main types of smart contracts on Ethereum platform:
  - Fungible tokens similar to stocks (ICOs based on ERC-20 protocol, 2017).
  - Non-fungible collectible tokens like CryptoKitties (2017) or NFTs (2020).
  - Digital identity management.
- All of the above can be implemented on top of Bitcoin using the **RGB protocol** within the Lightning Network, providing both **contract flexibility** and **scalability**.

Mining Centralization 1/2

- Bitcoin's Proof-of-Work system uses simple SHA-256d (double SHA-256) algorithm.
- SHA-256d can be easily implemented in specialized hardware (**ASICs - Application specific integrated circuits**.
- As of 2021, Bitcoin is mined solely on ASICs, as any generic purpose hardware is way to slow to be profitable.
- Bitcoin ASICs are mostly produced in China, which, combined with the low electricity costs, resulted in an accumulation of significant amounts of **hash-power** in mainland China.
- Some people within cryptocurrency community consider ASIC resistance to be an important characteristic of the "next generation" cryptocurrency system.

Mining Centralization 1/2

- Bitcoin's point of view:
  - ASICs are slowly approaching theoretical efficiency limits, so there is less incentive to install them close to the manufacturer (i.e. in China),
  - a decentralization tendency has been observed in the last several years - more mining operations are being set up in other countries,
  - that said, there are discussions of a potential change of the PoW algorithm in a distant future.

Energy Consumption

- Lately, Bitcoin is being aggressively criticized by the mainstream media for its total energy consumption.
- Most of the claims on Bitcoin's energy consumption show little to no understanding of both Bitcoin and electricity usage:
  - excess electricity cannot be stored,
  - miners are incentivized to put their equipment close to cheap excess electricity sources,
  - a consumer consumes too much electricity iff it causes electrical grid outages in the area where consumption occurs, otherwise it's just excess electricity consumption,
  - value proposition of Bitcoin far outweighs the costs of electricity consumed.
- This has been discussed in great details by Nic Carter on Twitter.

Proof of Stake

- **Proof of stake** (PoS) protocols are a class of consensus mechanisms for blockchains that work by selecting validators in proportion to their quantity of holdings in the associated cryptocurrency.
- The first functioning use of PoS for cryptocurrency was Peercoin in 2012.
- Proof of stake violates the energy-based interpretation of decentralized consensus: **Bitcoin blocks are secured by large amounts of energy needed to generate one**.
- "Proof of Stake is why Proof of Work was invented." - @notgrubles on Twitter.

Transaction Privacy 1/2

- Bitcoin block chain data is transparent: for every “chunk” of bitcoin created by a coinbase transaction, the whole transaction history can be followed by simply looking at the chain data.
- Bitcoin addresses are **pseudonymous**: outputs to the same address can be easily tied together.
- As a result, Bitcoin chain is susceptible to **chain analysis** that in some cases allows to establish the sender and the recipient of the bitcoin (the amount is publicly visible directly).
- This makes Bitcoin hard to use as a currency for daily payments, where transaction privacy is essential (salary, medication bills, etc).

Transaction Privacy 2/2

- Lightning Network significantly improves transaction privacy by moving most of the transactions off chain.
- Channel open and channel close transactions are still visible on chain.
- Proposals to implement privacy features on Bitcoin **sidechains**.

Case Study: Ethereum 1/2

- Created by Vitalik Buterin - a Russian-Canadian programmer and an active member of Bitcoin community in the early days.
- Launched in 2014.
- Main difference from Bitcoin: Turing-complete smart contract language Solidity with JavaScript-like syntax.
- In order to avoid the infinite loops and transaction spam, Ethereum's fee system requires users to pay for operations executed by their smart contracts - this is called **paying for gas**.

Case Study: Ethereum 2/2

- Turing-completeness of the Ethereum was the reason behind the infamous "DAO hack" - loss of a large amount of funds in 2016 that caused **the Ethereum governing body to revert a transaction via a hard fork**.
- An investigation in 2019 indicated that 60% of Ethereum nodes were running in the cloud on centralized platforms like AWS.
- Ethereum's scalability problem is even worse than that of Bitcoin: full archive is approximately 7.3 Tb of data, while the regular pruned node size is 300 Gb.
- Ethereum network is determined to move to a Proof-of-Stake system.

Case Study: Monero 1/2

- Based on the CryptoNote protocol described by a pseudonymous entity **Nickolas van Saberhagen**.
- Created by a pseudonymous individual **thankful_for_today** who forked the codebase of CryptoNote-based coin Bytecoin and launched the network.
- Similar to Bitcoin, has no central governing body.
- Very simple transaction structure with no scripting system.
- ASIC-resistant Proof-of-Work algorithm.
- Variable block size, short period between blocks (2 minutes).
- Protocol upgrades are performed via **planned hard forks**, which is only feasible because the network is comparatively small.

Case Study: Monero 2/2

- Based on the CryptoNote protocol described by a pseudonymous entity **Nicolas van Saberhagen**.
- Created by a pseudonymous individual **thankful_for_today** who forked the codebase of CryptoNote-based coin Bytecoin and launched the network.
- Has a very simple transaction structure with no scripting system.
- The privacy of Monero is achieved by concealing the following information:
  - the sender of the money via the **ring signatures**,
  - the receiver of the money via the **stealth addresses**,
  - the amount sent via the Confidential Transactions system that encrypts the amounts in transaction but allows to check that the amount spend is greater than the amount received.

Conclusions

- Bitcoin and Monero are the only cryptocurrencies whose creators are no longer engaging with the community.
- Satoshi Nakamoto never appeared online since 2011.
- Some people believe Satoshi disappeared to prevent any entity, including themselves, from manipulating the community using their name, identity, sentimental role, or the amount of bitcoin they presumably own.
- Bitcoin community is very conservative regarding the protocol changes, and network safety and stability are considered the most important goals.
- Features that Bitcoin lacks can often be implemented as layer-2 solutions.
- Transaction privacy is one of the first priority goals (after safety and stability).
- **Do we need other cryptocurrencies?**

The End

Thank you!