Bitcoin and Cryptocurrency Technologies
Lecture 9: Bitcoin Scaling 1/2

Yuri Zhykin

Apr 21, 2025

Transaction Throughput

- Block every 10 minutes (600 seconds).
- Every block - 1-1.5 Mb.
- Average transaction size - 500 bytes.
- Throughput

$$T = \frac{1.5 * 1024 * 1024}{500 * 600} \approx 5\text{tx/sec}$$

- Visa throughput is approx. 1700 tx/second.

Throughput Scaling Proposals

- **Increase block size** - more centralization; current chain size growth rate is 80 Gb/year.
- **Increase block frequency** - more centralization, less network stability.
- **Optimize transaction structure** - limited possibilities.
- **Second-layer solutions** - the only viable approach?

Transaction Structure Optimization

- **Segregated Witness** (**SegWit**).
- **Schnorr signatures**.
- **Merkelized Abstract Syntax Trees** (**MAST**).
- **Taproot** (both **Schnorr** and **MAST**).

SegWit 1/4

- Protocol upgrade that was activated in 2017 and solved the following problems:
  - **transaction malleability** - for a non-SegWit transaction it is possible to change the transaction in a way that changes the transaction ID (hash) while the signature remains valid;
  - **block space optimization** - no need to store the usually large unlock script in the block - it is moved into a Witness structure;
  - **future upgrades** - SegWit introduced a clean way for upgrading the protocol via **softforks**.

SegWit 2/4

- SegWit followed the idea of P2SH (BIP-0016) - additional script validation rules based on the pattern in the script.
- Main transaction components are now **inputs**, **outputs** and **witnesses** (one **witness** per **input**).
- For every transaction input, if **lock-script** *being executed* is a **witness program**
  - take the **witness** structure,
  - verify that the **witness program** matches the hash of the **witness** structure,
  - interpret **witness** structure as an **unlock-script**.

SegWit 3/4

- **P2WPKH** - pay-to-witness-public-key-hash
  - Lock: `0 <20-byte-key-hash>;`
  - Unlock: `;`
  - Witness: `<signature> <pubkey>`
- **P2WSH** - pay-to-witness-script-hash
  - Lock: `0 <32-byte-key-hash>;`
  - Unlock: `;`
  - Witness: `0 <signature1> 1 <pubkey1> <pubkey2> 2 CHECKMULTISIG>`
- **P2SH-P2WPKH** - P2WPKH nested in BIP16 P2SH
  - Lock: `HASH160 <20-byte-script-hash> EQUAL;`
  - Unlock: `<0 <20-byte-key-hash>>;`
  - Witness: `<signature> <pubkey>`
- **P2SH-P2WSH** - P2WSH nested in BIP16 P2SH
  - Lock: `HASH160 <20-byte-hash> EQUAL;`
  - Unlock: `<0 <32-byte-key-hash>>;`
  - Witness: `0 <signature1> 1 <pubkey1> <pubkey2> 2 CHECKMULTISIG>`

SegWit 4/4

- Witness structures are included in the block chain via the **witness root hash**, which is recorded in a **lock-script** of the **coinbase** transaction.
- **Witness root hash** is the *merkle root* of the *merkle tree* of the **wtxid**s:

  `txid`: `[nVersion][txins][txouts][nLockTime]`

  `wtxid`: `[nVersion][marker][flag][txins][txouts][witness][nLockTime]`

- Block size restriction $(1,000,000)$ is changed as follows:
  - *BlockWeight* is defined as $\mathit{BaseSize} * 3 + \mathit{TotalSize}$;
  - *BaseSize* is the block size in bytes with the original transaction serialization without any witness-related data;
  - *TotalSize* is the block size in bytes with transactions serialized as described in BIP144, including base data and witness data;
  - The new rule is $\mathit{BlockWeight} \leq 4,000,000$.

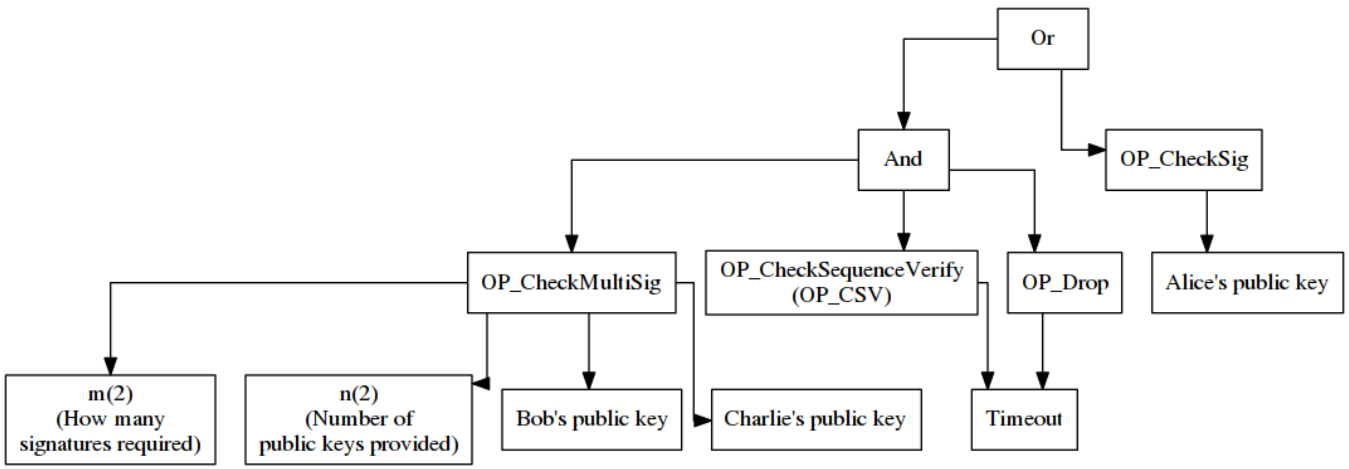
Schnorr Signatures

- **Schnorr signature** is an alternative cryptographic signature scheme that provides certain properties that are desirable for the Bitcoin system, e.g. **linearity** that allows for key/signature aggregation:

$$key_x = key_1 + key_2 + ... + key_n$$
$$sig_x = sig_1 + sig_2 + ... + sig_n$$

MAST and Taproot

- **Merkelized Abstract Syntax Trees** (**MAST**) is an way to support large complex scripts in Bitcoin by building a *merkle tree* from it and only revealing the **tree path** used for unlocking, enhansing privacy.



- Both **Schnorr signatures** and a variation of **MAST** are part of the **Taproot** soft-fork that activated on the mainnet on November 14, 2021.

Recommended Resources

- **Bitcoin: A Work in Progress**
  - book by Sjors Provoost, Bitcoin Core contributor
  - https://btcwip.com

The End

Thank you!