CMPSC 390
Blockchain Scalability.

Janyl Jumadinova

February 4, 2021
Scalability Problem

Goal:
Provide all of the services that a blockchain offers to all users, independent of how many users there are.
Layer 1 vs. Layer 2

Layer 1:
- refers to the main blockchain architecture
- the Bitcoin Blockchain, the Ethereum Blockchain
Layer 1 vs. Layer 2

Layer 1:
- refers to the main blockchain architecture
- the Bitcoin Blockchain, the Ethereum Blockchain

Layer 2:
- refers to a secondary framework or protocol that is built on top of an existing blockchain
- the Lightning Network, Ethereum Plasma
Taproot (Layer 1)

https://www.coindesk.com/taproot-merged-bitcoin-core

Problems:
Signature verification is slow, but required everywhere in the network.
Users can see many details of a transaction (all scripts, multisignature, etc.)

Taproot + Schnorr
Schnorr is a type of signature, Taproot is the Bitcoin upgrade (BIP) that uses Schnorr.

Idea:
If signature validation is faster, much of the network can run faster (more throughput).
Taproot replaces ECDSA signatures with Schnorr Signatures.
Taproot (Layer 1)

https://www.coindesk.com/taproot-merged-bitcoin-core

Problems:

- Signature verification is slow, but required everywhere in the network.
- Users can see many details of a transaction (all scripts, multisignature, etc.)
Taproot (Layer 1)

https://www.coindesk.com/taproot-merged-bitcoin-core

Problems:
- Signature verification is slow, but required everywhere in the network.
- Users can see many details of a transaction (all scripts, multisignature, etc.)

Taproot + Schnorr
- Schnorr is a type of signature, Taproot is the Bitcoin upgrade (BIP) that uses Schnorr.
Taproot (Layer 1)

https://www.coindesk.com/taproot-merged-bitcoin-core

Problems:
- Signature verification is slow, but required everywhere in the network.
- Users can see many details of a transaction (all scripts, multisignature, etc.)

Taproot + Schnorr

- **Schnorr** is a type of signature, **Taproot** is the Bitcoin upgrade (BIP) that uses Schnorr.
- **Idea**: If signature validation is faster, much of the network can run faster (more throughput).
Taproot (Layer 1)

https://www.coindesk.com/taproot-merged-bitcoin-core

Problems:

- Signature verification is slow, but required everywhere in the network.
- Users can see many details of a transaction (all scripts, multisignature, etc.)

Taproot + Schnorr

- **Schnorr** is a type of signature, **Taproot** is the Bitcoin upgrade (BIP) that uses Schnorr.
- **Idea**: If signature validation is faster, much of the network can run faster (more throughput).
- Taproot replaces ECDSA signatures with Schnorr Signatures.
Benefits of Taproot + Schnorr

*Key aggregation:*

- Multiple signers create an aggregate public key and an aggregate signature.
Benefits of Taproot + Schnorr

Key aggregation:

- Multiple signers create an aggregate public key and an aggregate signature.
- Multisig looks and costs the same as a single signature.
**Benefits of Taproot + Schnorr**

*Key aggregation:*

- Multiple signers create an aggregate public key and an aggregate signature.
- Multisig looks and costs the same as a single signature.
- 30 – 75% savings.
Benefits of Taproot + Schnorr

**Key aggregation:**
- Multiple signers create an aggregate public key and an aggregate signature.
- Multisig looks and costs the same as a single signature.
- 30 – 75% savings.

**Batch validation:**
- Many signatures can be verified at once.
Benefits of Taproot + Schnorr

*Key aggregation:*
- Multiple signers create an aggregate public key and an aggregate signature.
- Multisig looks and costs the same as a single signature.
- 30 – 75% savings.

*Batch validation:*
- Many signatures can be verified at once.
- Speedup grows logarithmically with the number of sigs to verify.
Benefits of Taproot + Schnorr

Key aggregation:
- Multiple signers create an aggregate public key and an aggregate signature.
- Multisig looks and costs the same as a single signature.
- 30 – 75% savings.

Batch validation:
- Many signatures can be verified at once.
- Speedup grows logarithmically with the number of sigs to verify.
- When a transaction has many scripts, they do not need to be revealed or evaluated on the network.
Segregated Witness (Layer 1)

https://blockchainhub.net by Valentik Kalinov

"SegWit means separating signatures out of transactions and keeping separated data repository of the signatures and making them optional in the propagation and storage."

What does it mean for Bitcoin?

It is a soft fork!

This is how a normal bitcoin transaction looks like

Bob sends money to Alice

Transaction message

Signature

Signatures prove if a transaction is authorized
Segregated Witness

SegWit separates the signature from the transaction

Bob → Transaction message + Signature → Alice

Signatures can be handled separately instead of the single chunk of data
Segregated Witness

A new style block with increased size limit to 4MB

Free space

Since signature data (witness data) is stored outside the transaction (and outside the standard block), it means that that data doesn’t have to be counted towards the block size

More transactions could be stored in a block, thus improving scalability
Sharding:

Do not require every miner to be working on every single block, essentially creating parallel but connected blockchains.

Ref.:
https://eth.wiki/sharding/Sharding-FAQs
Sharding:

Do not require every miner to be working on every single block, essentially creating parallel but connected blockchains.

Ref.: https://eth.wiki/sharding/Sharding-FAQs
Lightning Network (Layer 2)

https://lightning.network/
Lightning Network (Layer 2)

https://lightning.network/

Lightning Network

Do not put every transaction on the blockchain.
Lightning Network (Layer 2)

https://lightning.network/

Lightning Network

Do not put every transaction on the blockchain.

**Payment Channel**

<table>
<thead>
<tr>
<th>Alice and Bob's Balance Sheet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
</tr>
<tr>
<td>10 BTC</td>
</tr>
</tbody>
</table>

Alice and Bob make several private txns.

<table>
<thead>
<tr>
<th>Alice and Bob's Balance Sheet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
</tr>
<tr>
<td>3 BTC</td>
</tr>
</tbody>
</table>
Lightning Network

https://lightning.network/

Lightning Network

Open Payment Channel

Blockchain Settlement When Payment Channel Closes
Ethereum 2.0

Multi-year timeline.

- **Phase 0**: Transition to Proof of Stake.
- **Phase 1**: Data Sharding.
- **Phase 2**: State + Execution (computation and smart contracts).
- **Phase 3+**: Other scaling solutions.