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

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:

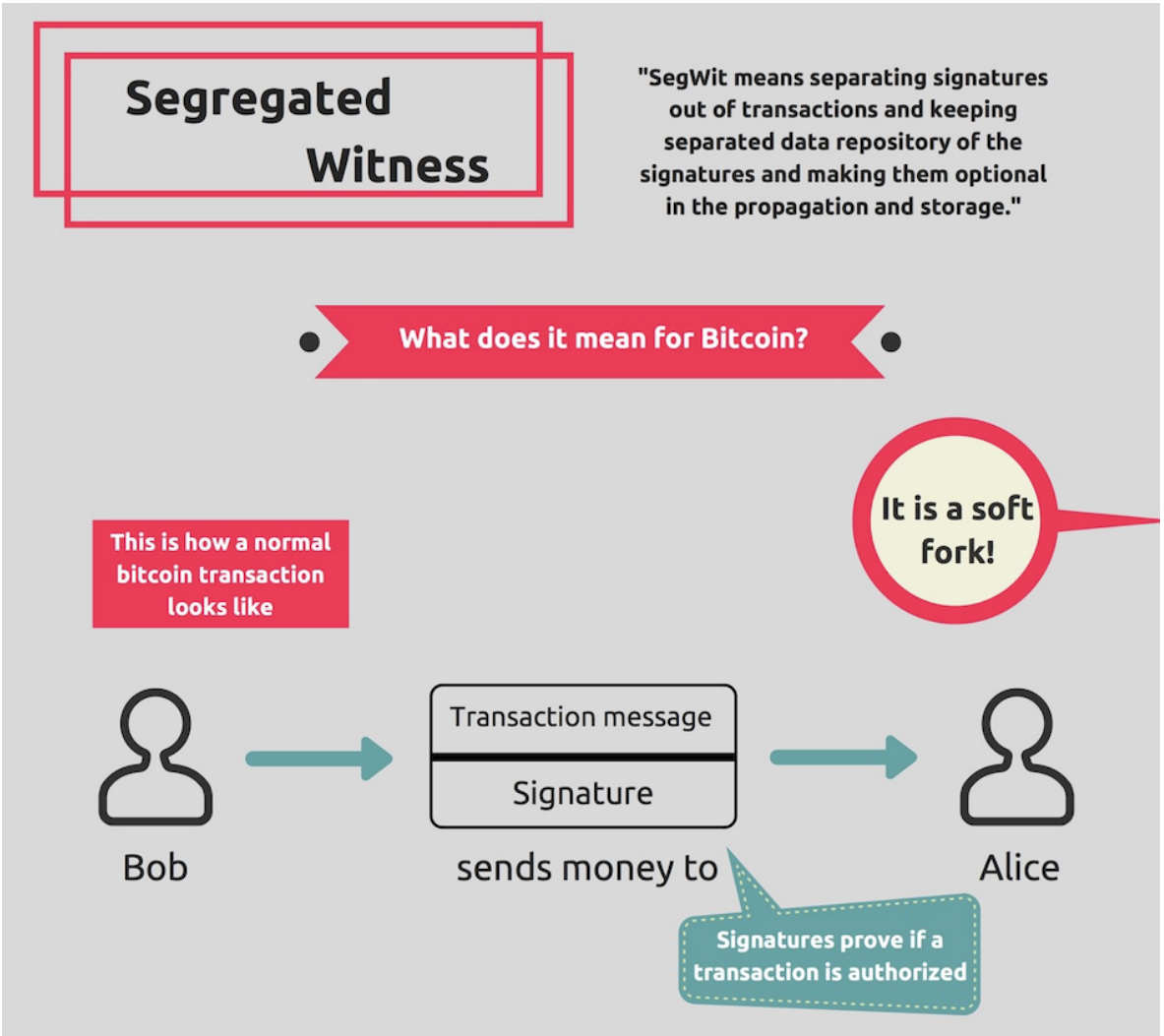
- Multiple signers create an aggregate public key and an aggregate signature.
- Multisig looks and costs the same as a single signature.
- $30 - 75\%$ savings.

Batch validation:

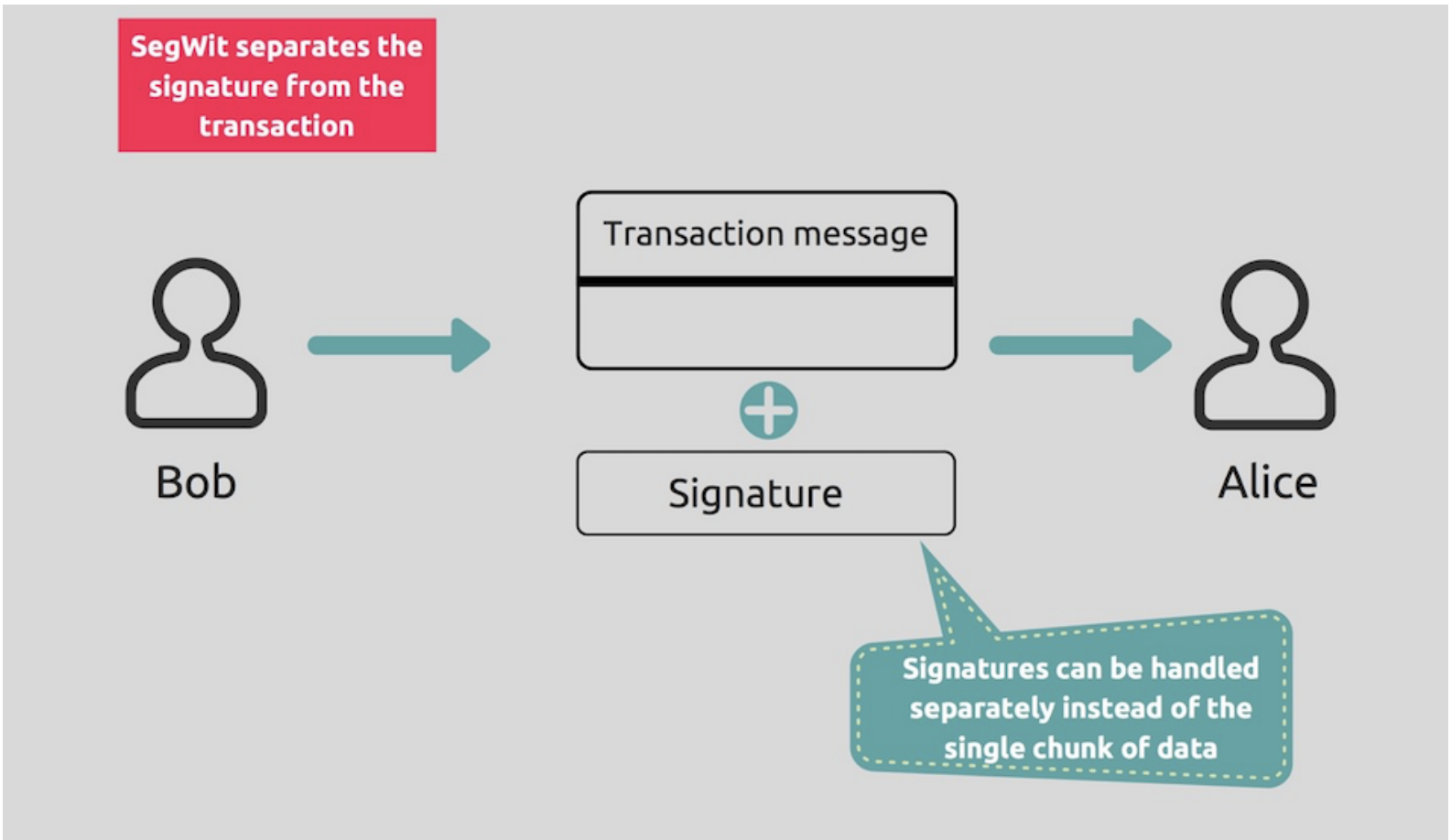
- Many signatures can be verified at once.
- Speedup grows logarithmically with the number of sigs to verify.
- When a transaction has many scripts, they do not need to be revealed or evaluated on the network.

Segregated Witness (Layer 1)

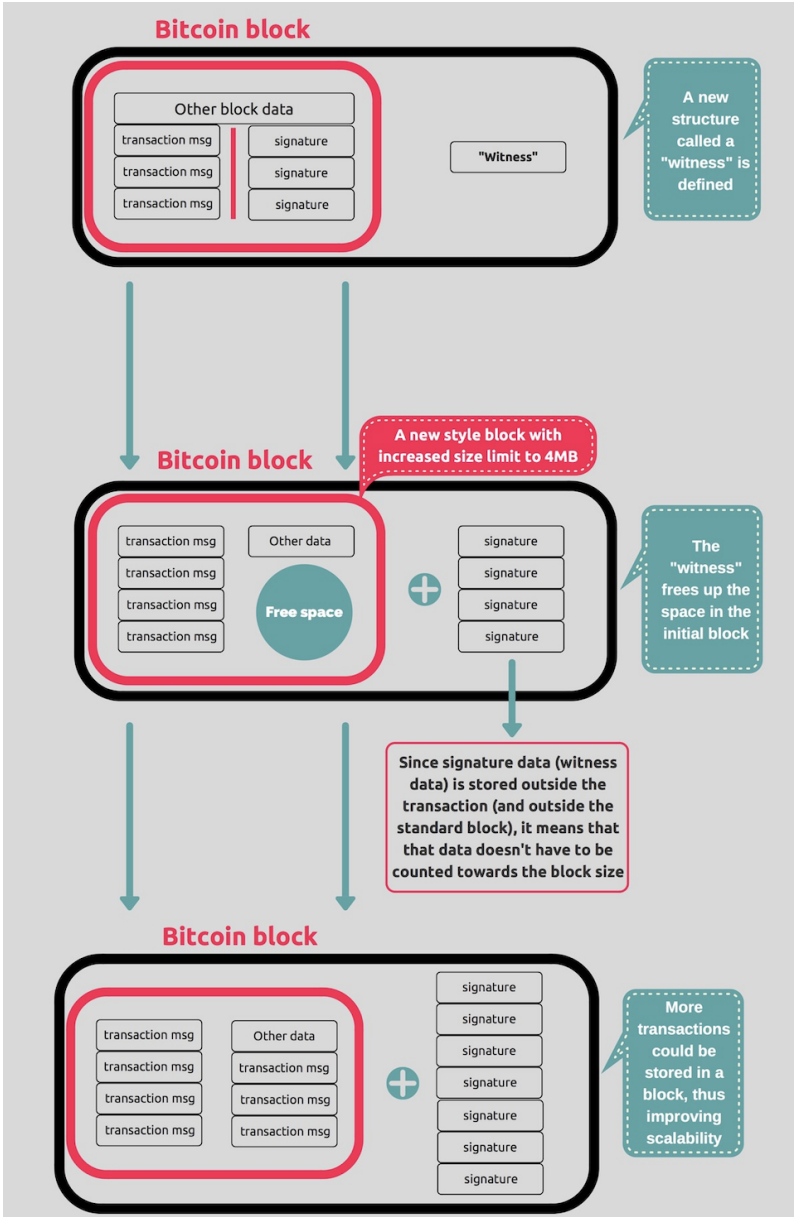
https://blockchainhub.net by Valentik Kalinov



Segregated Witness



Segregated Witness



Sharding

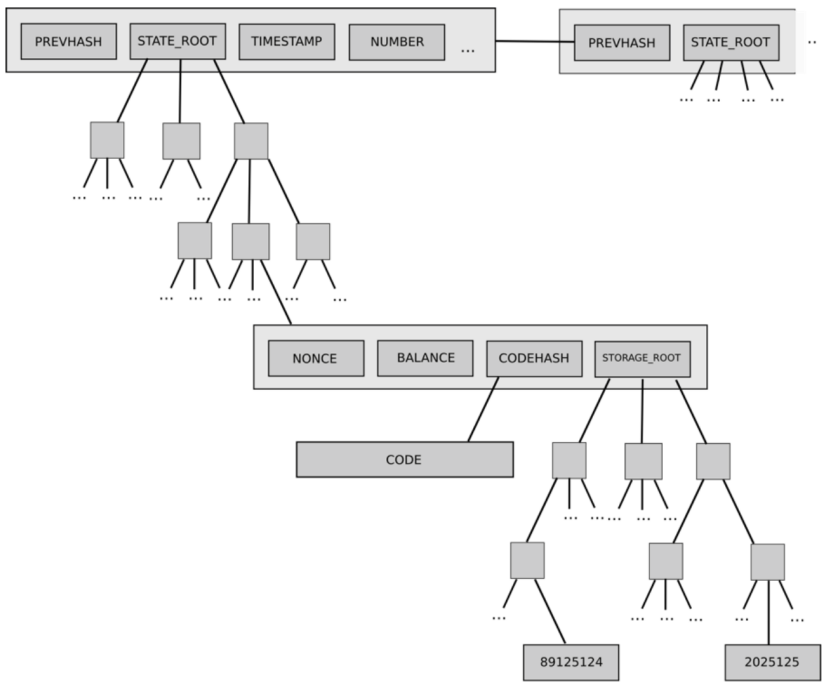
Sharding:

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

Sharding

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

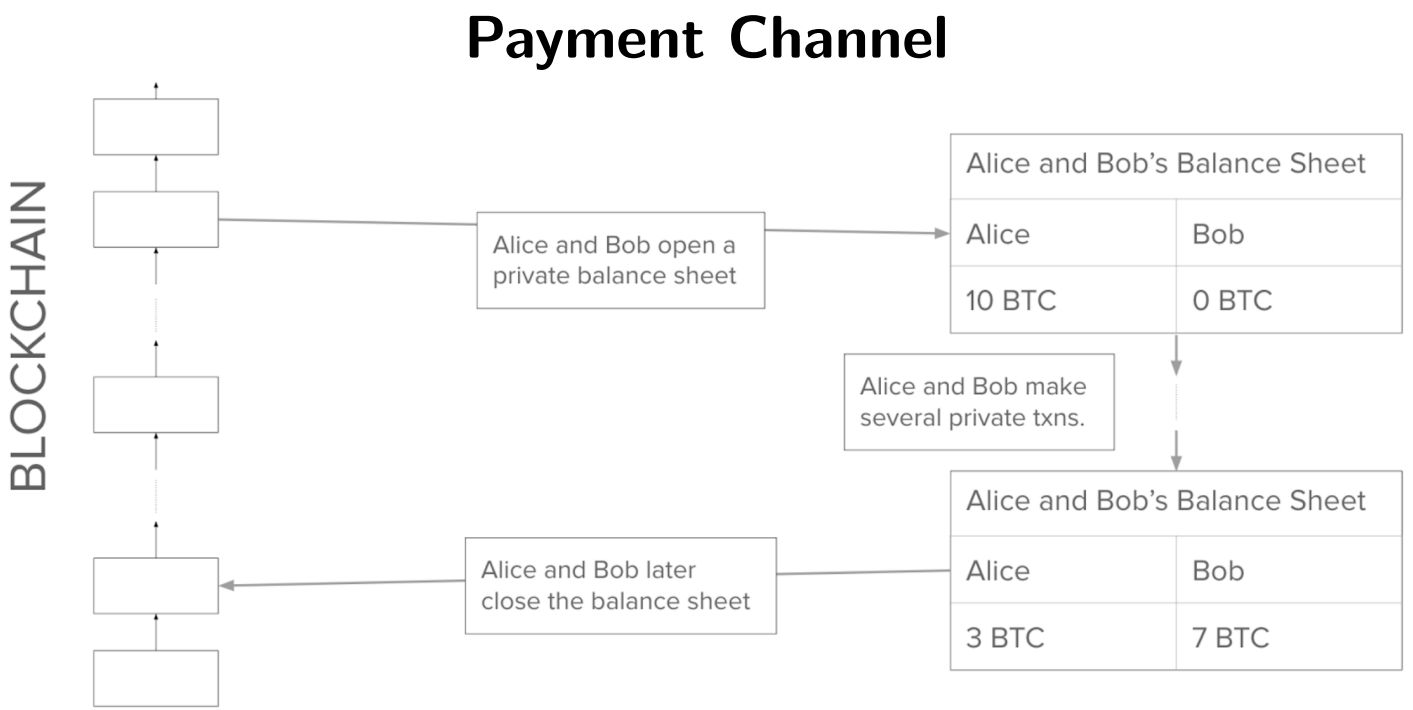
Do not put every transaction on the blockchain.

Lightning Network (Layer 2)

https://lightning.network/

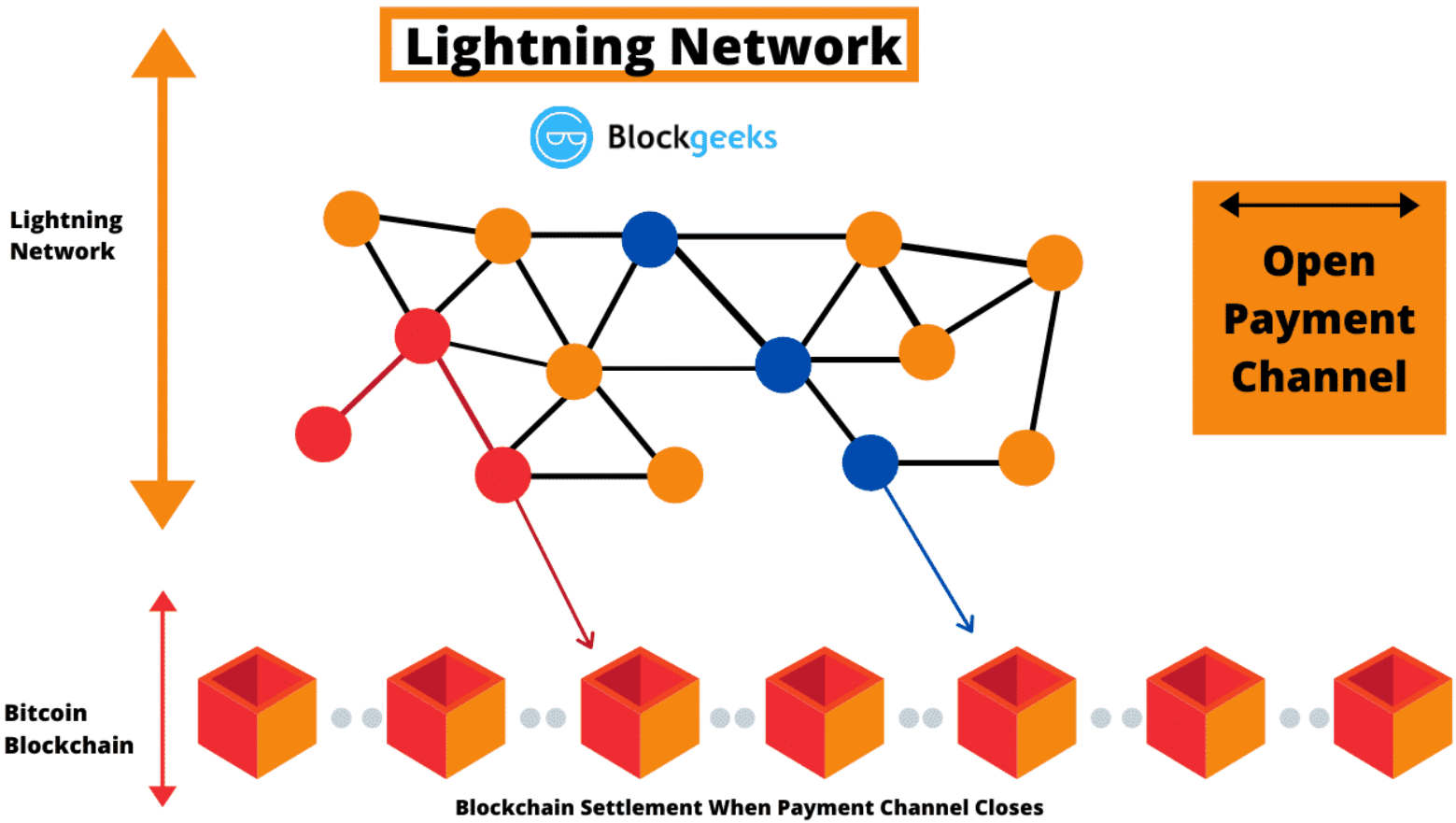
Lightning Network

Do not put every transaction on the blockchain.



Lightning Network

https://lightning.network/



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.