

iroh p2p connections

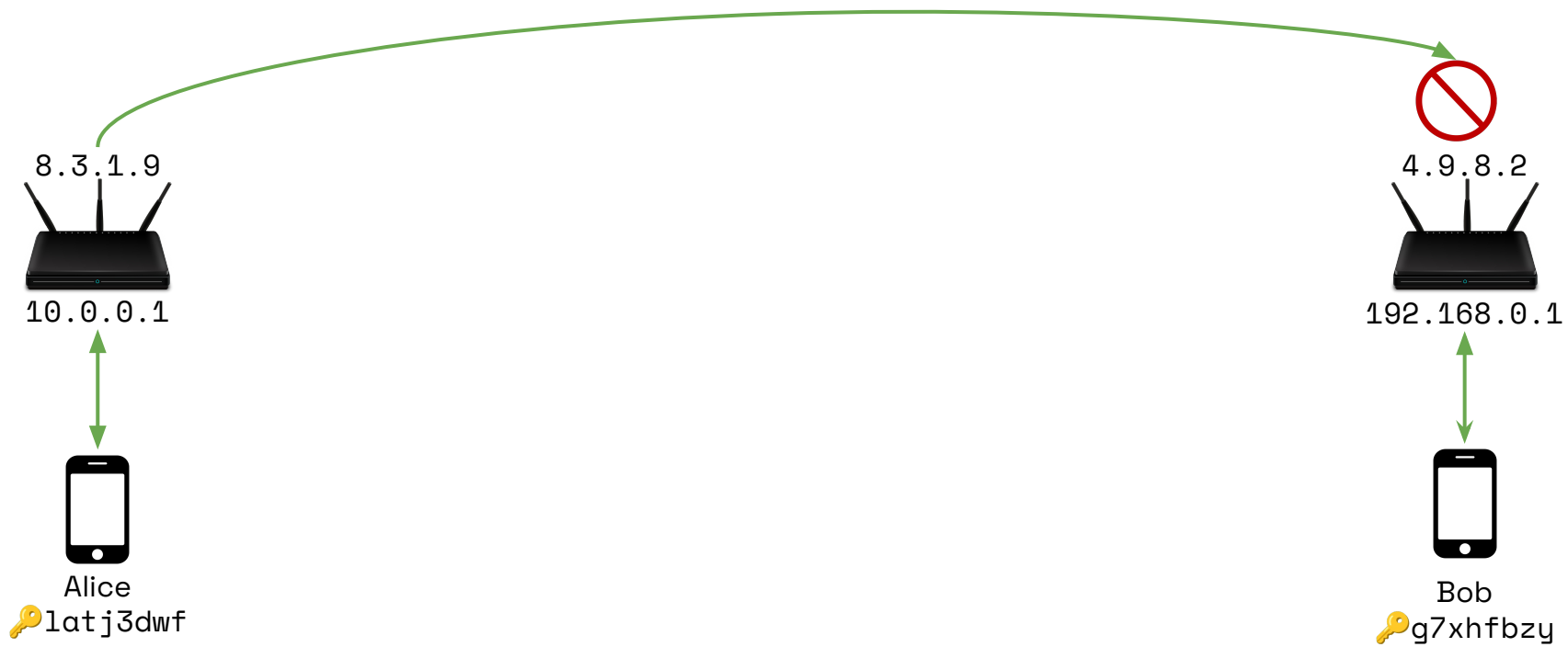
Floris Bruynooghe

number 0

<https://mastodon.social/@flub>

<https://mastodon.social/@n0iroh>

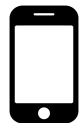
iroh is a library for ***direct* QUIC** connections between
nodes **identified** and **encrypted** using **ed25519**
keypairs



Server (us-east-1)

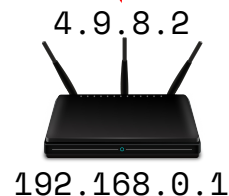


This makes me 🙄



Alice

🔑 latj3dwf



Bob

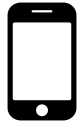
🔑 g7xhfbzy

iroh Relay Server

HTTPS
→ WebSocket

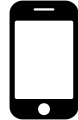
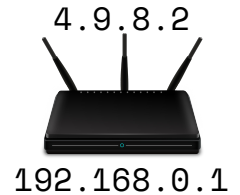


direct IP



Alice

🔑 1atj3dwf

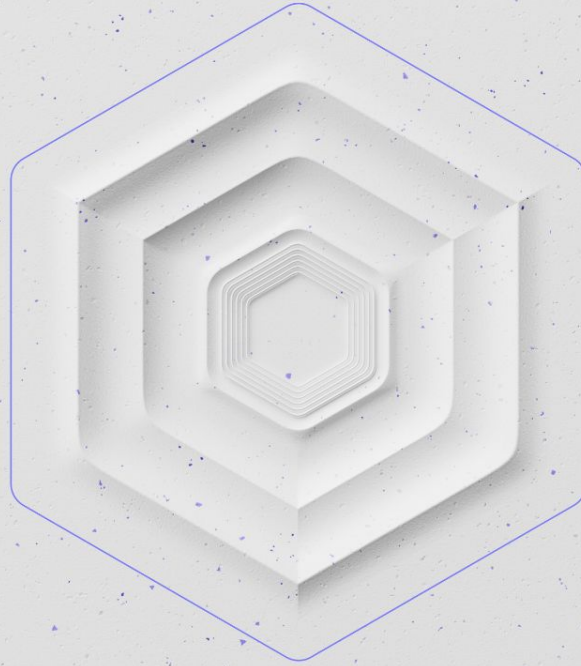


Bob

🔑 g7xhfbzy

Dial by Endpoint ID

who, not *where*



Address Lookup

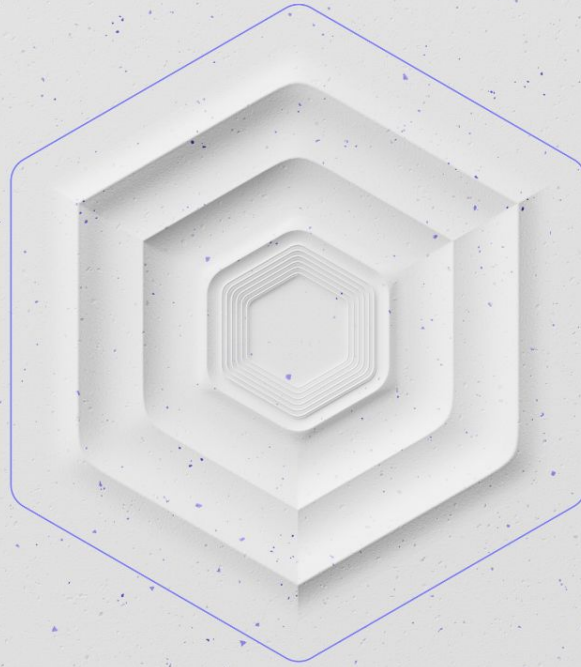
Endpoint ID

- Relay URL
- IP Address

- DNS
 - pkarr publisher
- mDNS
 - local network
 - extra: discover neighbours
- DHT
 - bittorrent mainline
 - pkarr
- <your own>
 - extensible

QUIC

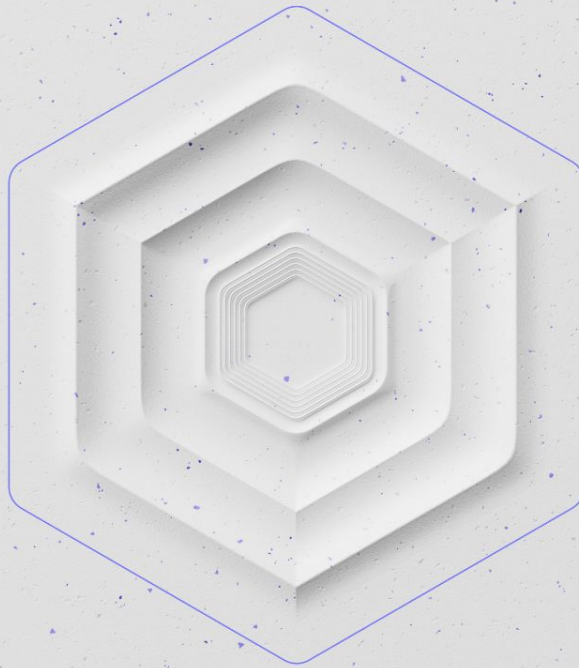
modern transport
protocol



QUIC

- **Streams** for reliable delivery
- Stream **multiplexing**, no head of line blocking
- **Datagrams** extension
- Encryption via **TLS**
- **1-rtt** or **0-rtt** handshake
- Loss detection & Congestion control
- Header encryption to prevent middlebox interference
- Extensible

Build Modular Protocols on QUIC



iroh-blobs

Request data **by hash**

Verified Streaming

iroh-gossip

Broadcast to the group

No central membership

iroh-blobs

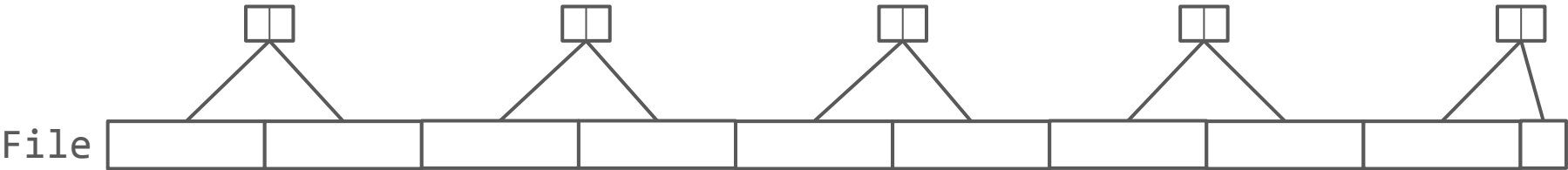
Verified streaming
using BLAKE3

[illegible]

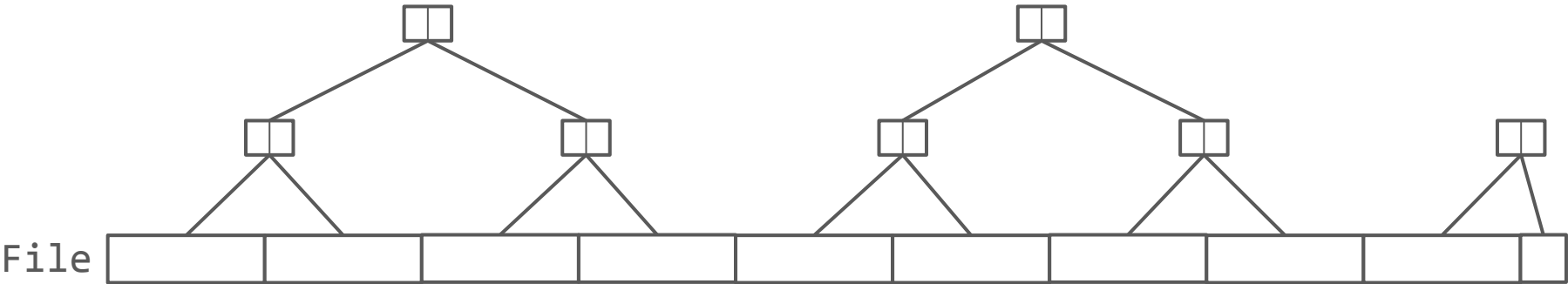
File

[illegible]

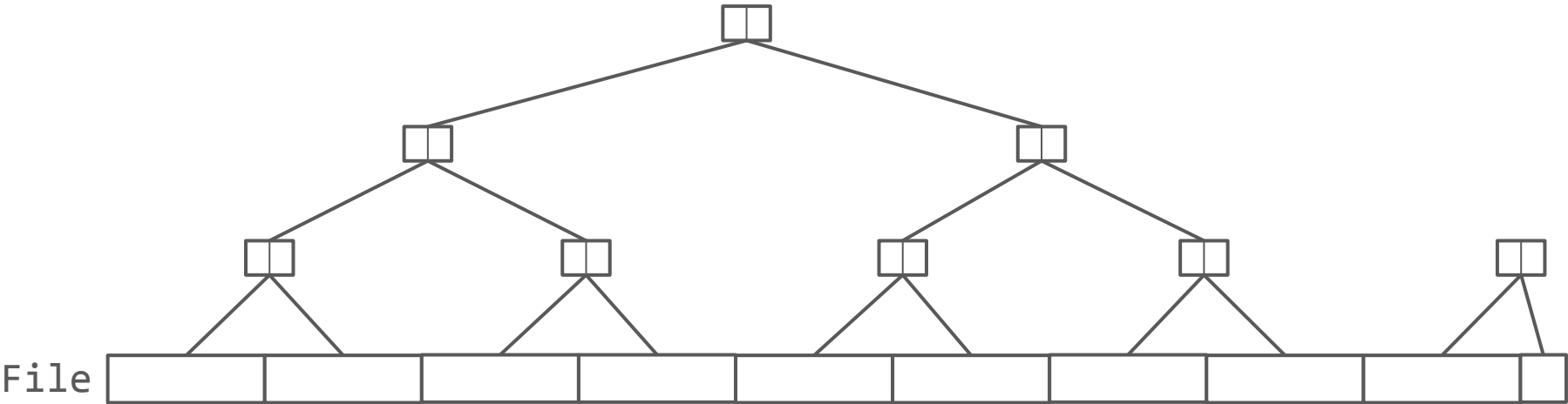
How does BLAKE3 work



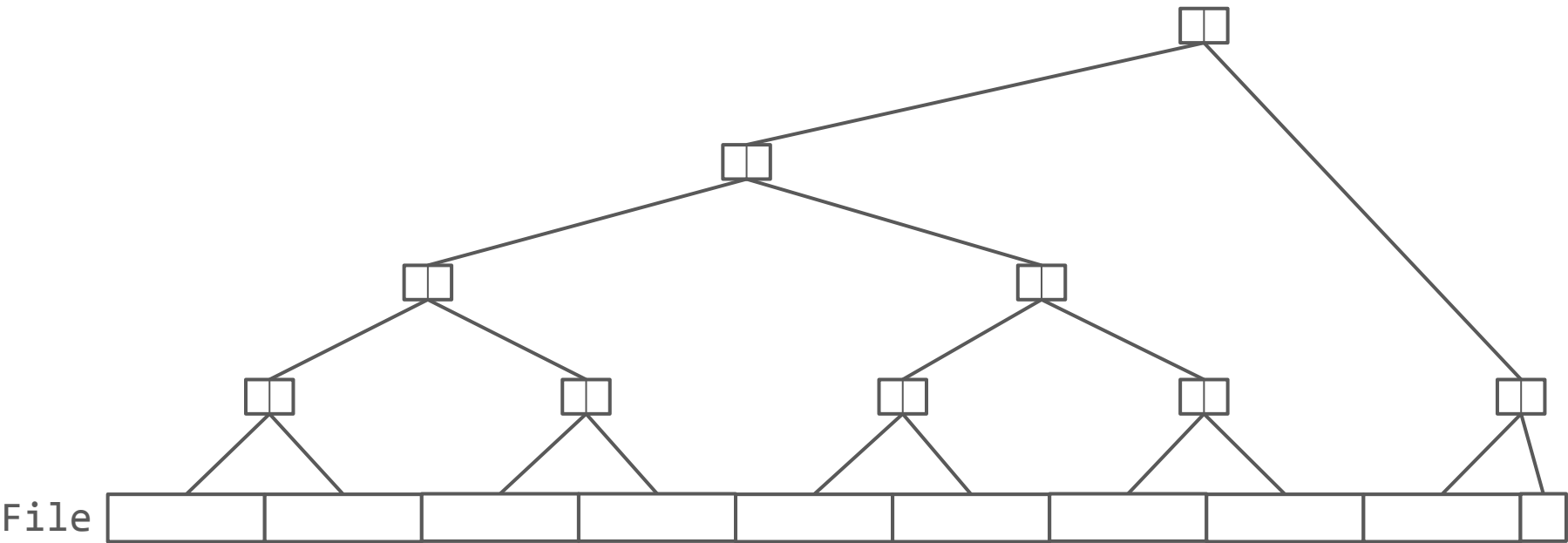
How does BLAKE3 work



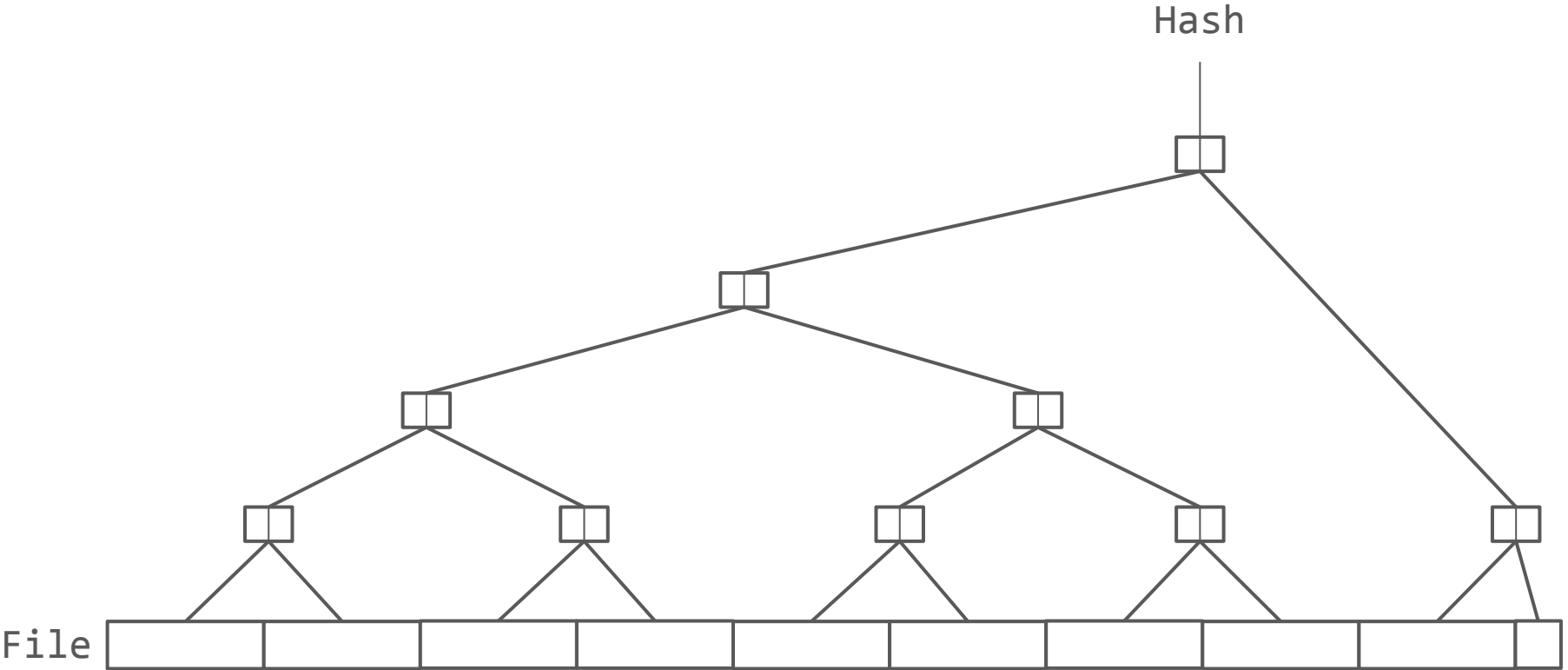
How does BLAKE3 work



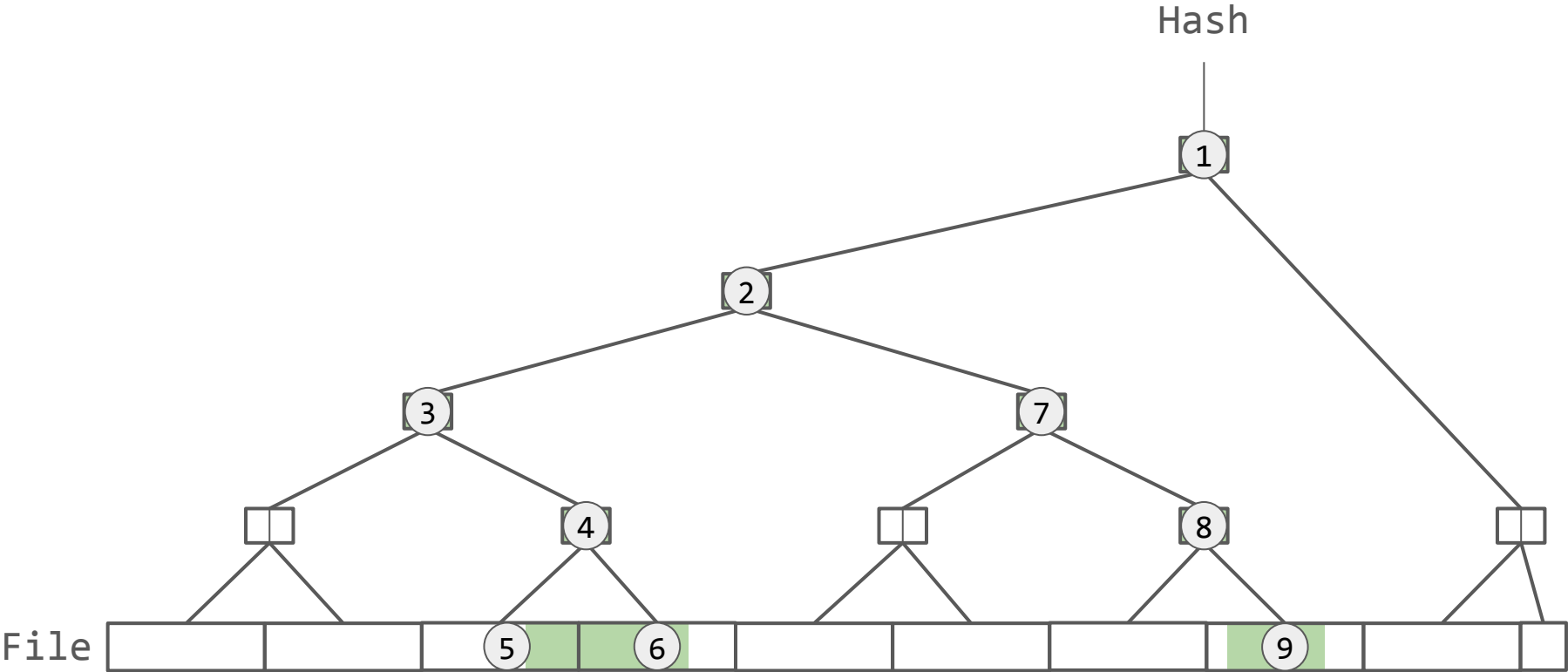
How does BLAKE3 work



How does BLAKE3 work



Verified encoding of ranges



iroh-gossip

- Epidemic broadcast trees
 - Share small messages to everyone
- Based on:

HyParView & PlumTree
- Built on p2p QUIC connections

HyParView

Hybrid Partial View

- Active neighbours
- Passive neighbours

PlumTree

Spanning Tree

- Prune redundant links
- Repair broken links

Thanks!

<https://iroh.computer>

<https://mastodon.social/@flub>

<https://mastodon.social/@n0iroh>

