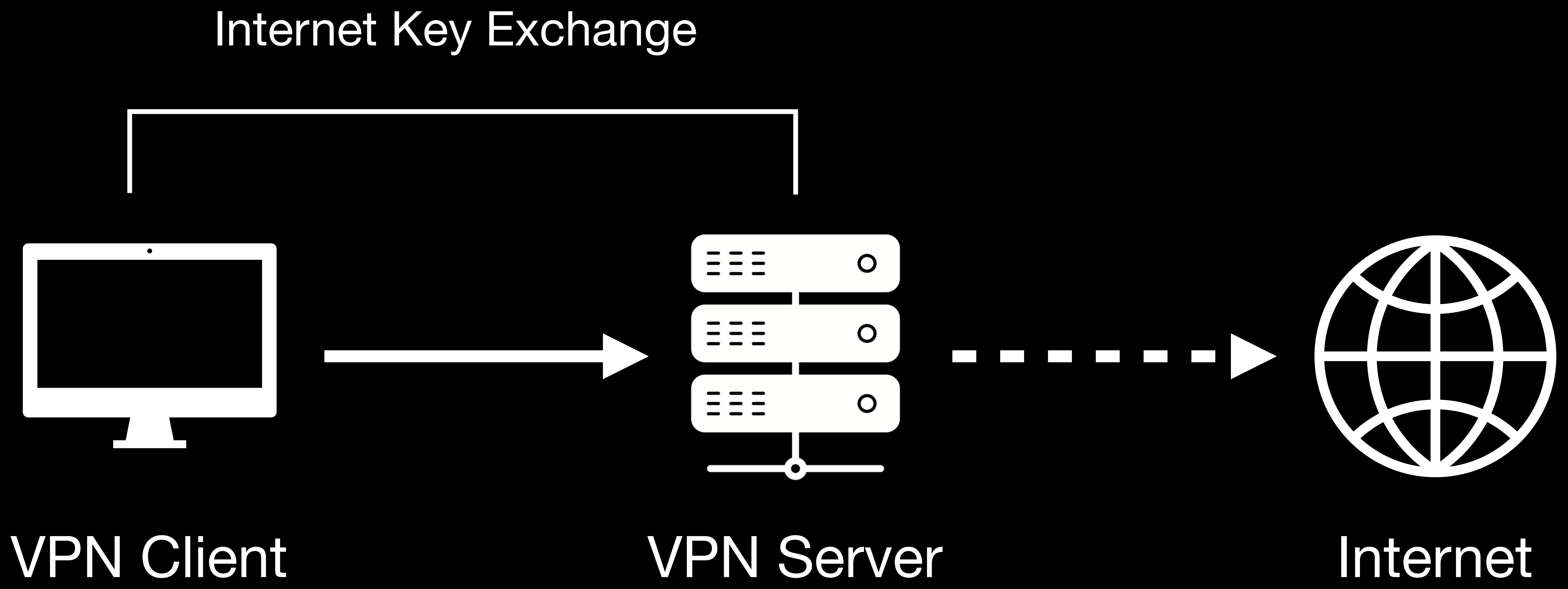
Beyond VPN and TOR: Protect Your Privacy with Decentralized Mixnets

Alexis Cao
@alexiscao.bsky.social

```
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100    13  100    13    0     0     13      0  0:00:01 --:--:--  0:00:01    13

 _ __  _   _ _ __ ___
| '_ \| | | | '_ ` _ \
| | | | |_| | | | | | |
|_| |_|\__, |_| |_| |_|
       |___/

        (mixnode - version 0.10.0)


Initialising mixnode winston-smithnode ...
 2021-04-17T02:38:21.113Z WARN  nym_mixnode::commands::init > one of bonded mixnodes is on invalid layer 1789
Saved mixnet identity and sphinx keypairs
Saved configuration file to "[redacted]/.nym/mixnodes/winston-smithnode/config/config.toml"
Mixnode configuration completed.



To bond your mixnode you will need to provide the following:
    Identity key: [redacted]
    Sphinx key: [redacted]
    Host: [redacted]
    Layer: 3
    Location: [physical location of your node's server]
    Version: 0.10.0


┌──([redacted])-[~/nym/target/release]
└─$ 
```

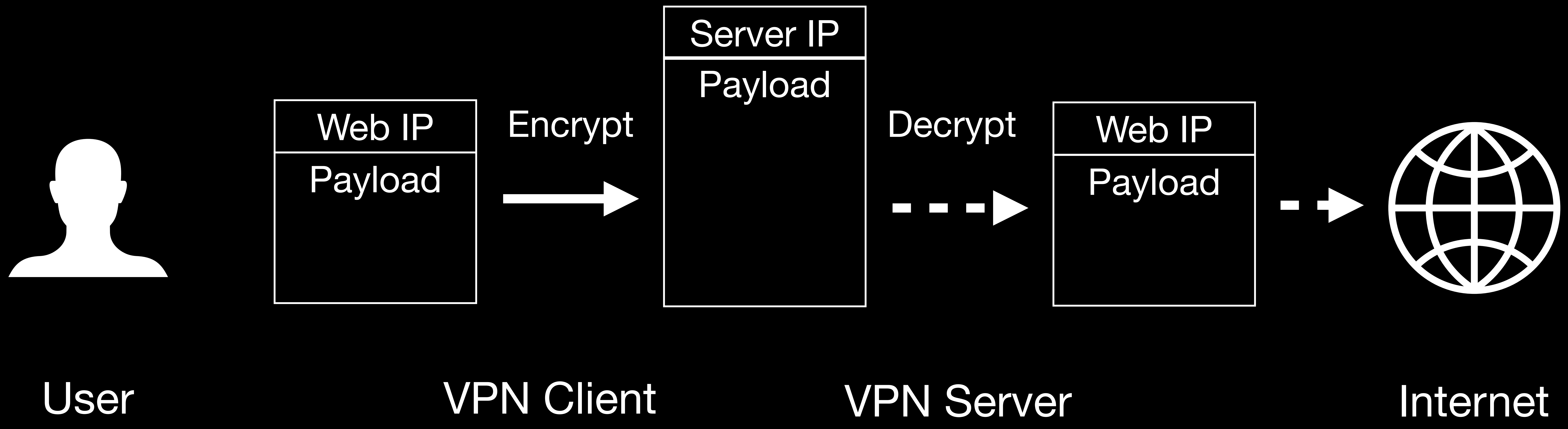


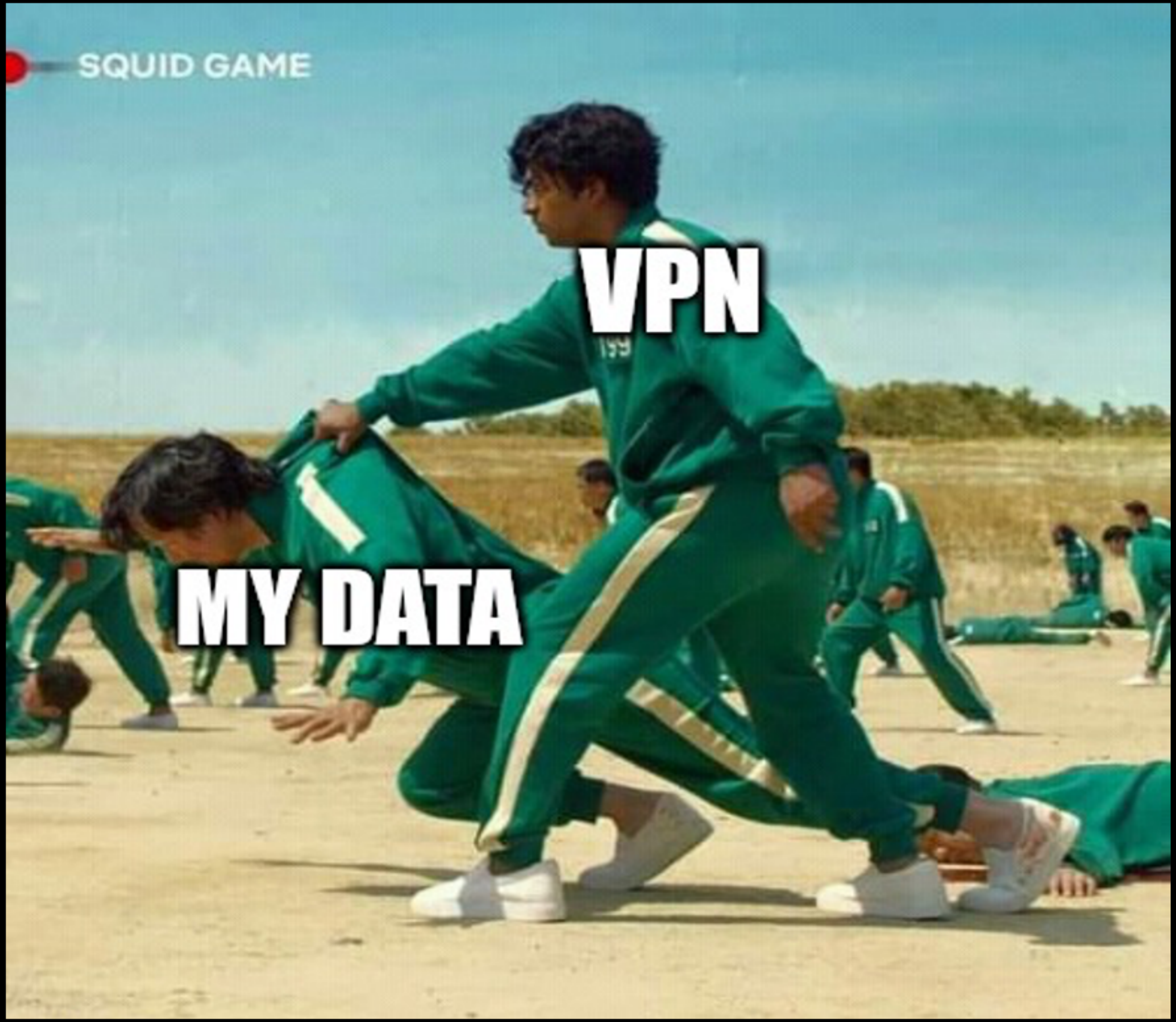
Internet Key Exchange

VPN Client

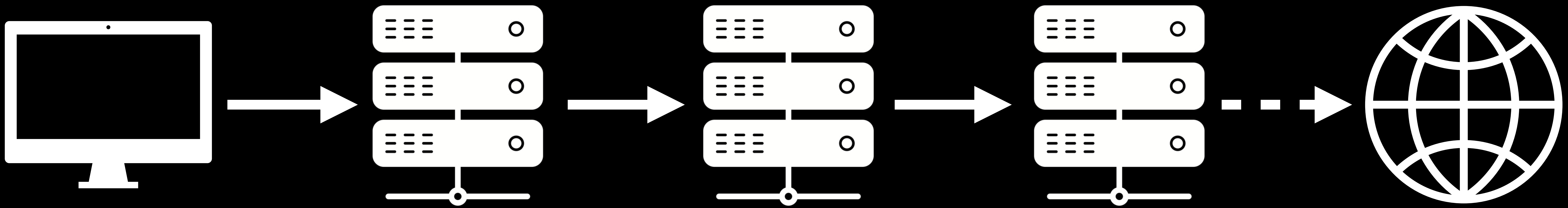
VPN Server

Internet


Web IP
Payload
Encrypt
Server IP
Payload
Decrypt
Web IP
Payload
User
VPN Client
VPN Server
Internet



https://turbovpn.com/blog/the-best-15-funny-vpn-memes



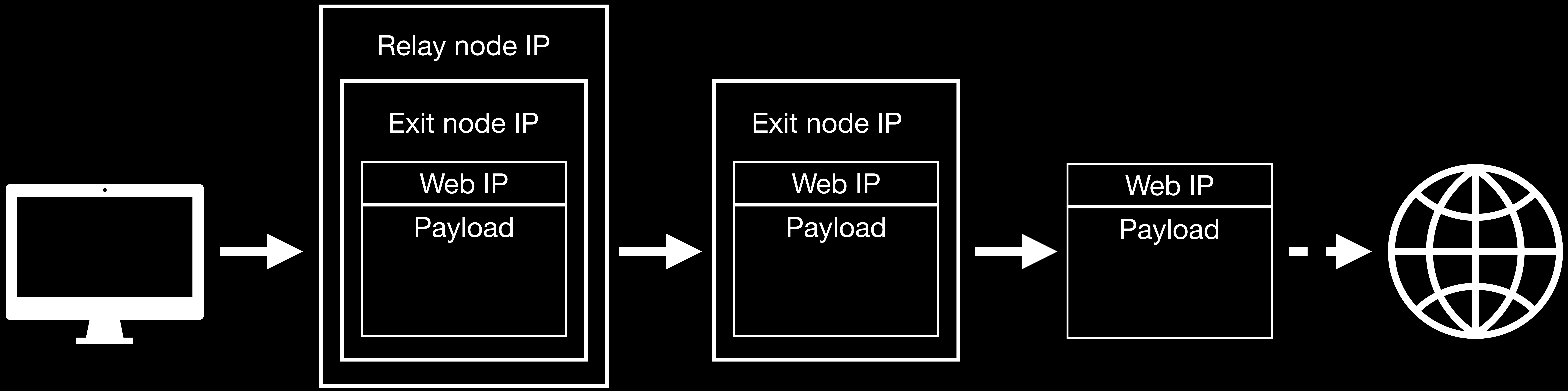
Tor Client

Entry Node

Relay Node

Exit Node

Internet



Relay node IP

Exit node IP

Web IP

Payload

Exit node IP

Web IP

Payload

Web IP

Payload

Tor Client

Entry node

Relay node

Exit node

Internet

Why not Tor?

Incentives for running nodes

+

Costs for running nodes

Other Decentralized Mixnets

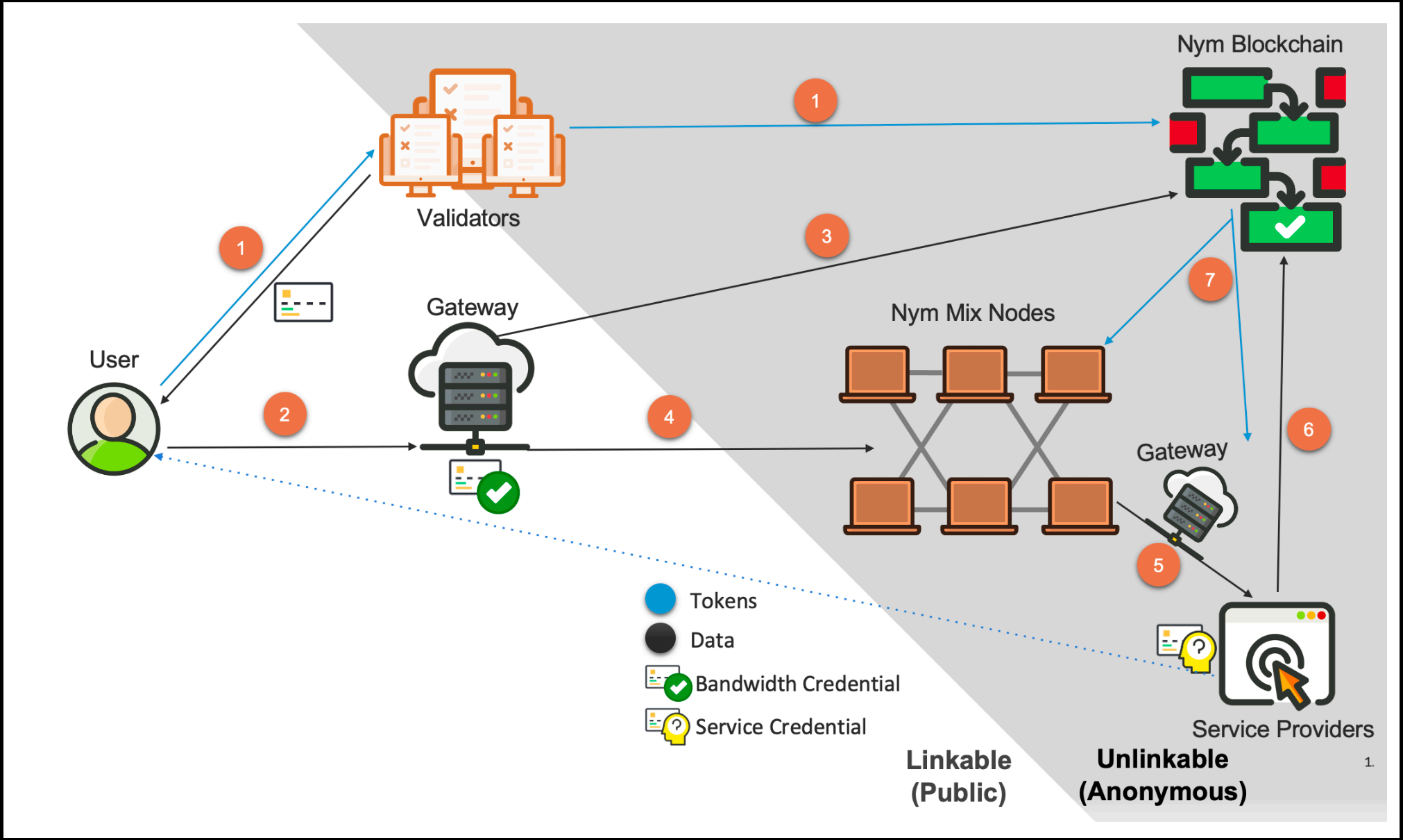
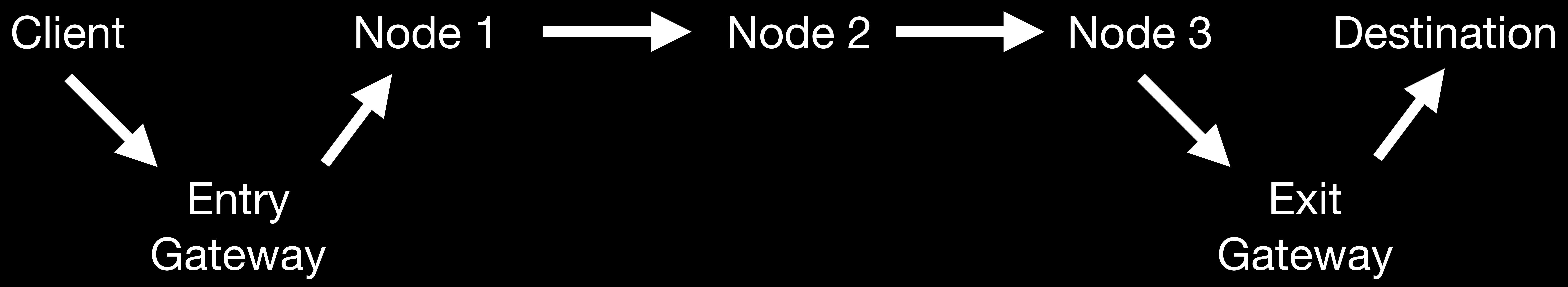


*figure from Nym whitepaper



Client

Entry Gateway

Node 1

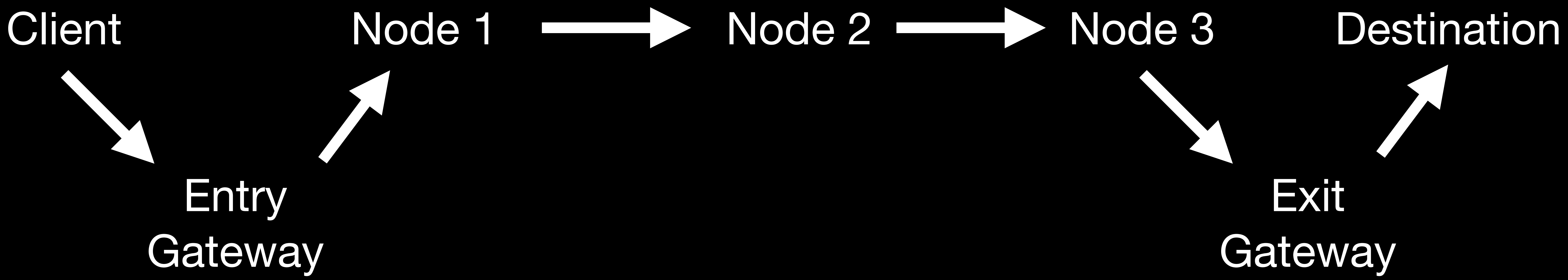
Node 2

Node 3

Exit Gateway

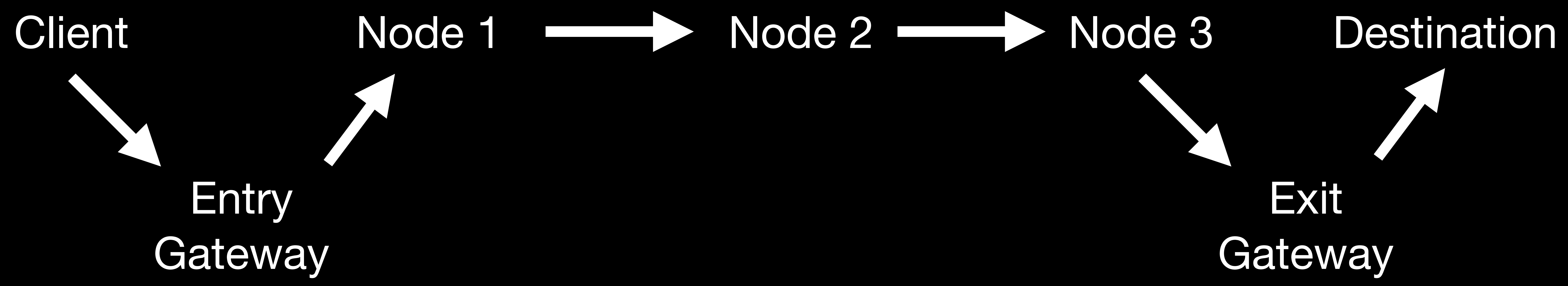
Destination

continuous-time mixing



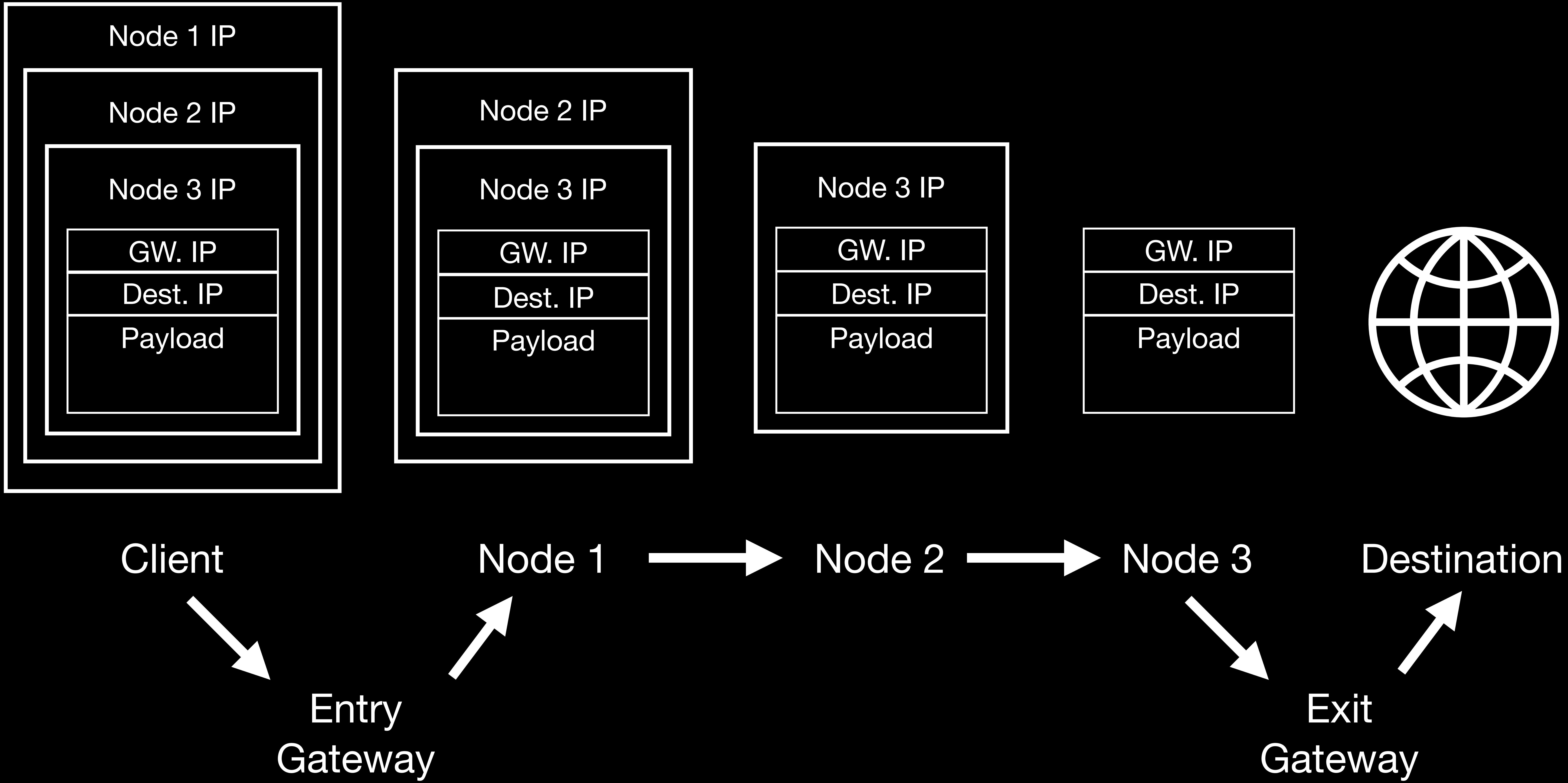
cover traffic

unlinkability + unobservability



layered network topology

Sphinx Packet Format



Node 1 IP

Node 2 IP

Node 3 IP

GW. IP

Dest. IP

Payload

Node 2 IP

Node 3 IP

GW. IP

Dest. IP

Payload

Node 3 IP

GW. IP

Dest. IP

Payload

GW. IP

Dest. IP

Payload

Client

Node 1

Node 2

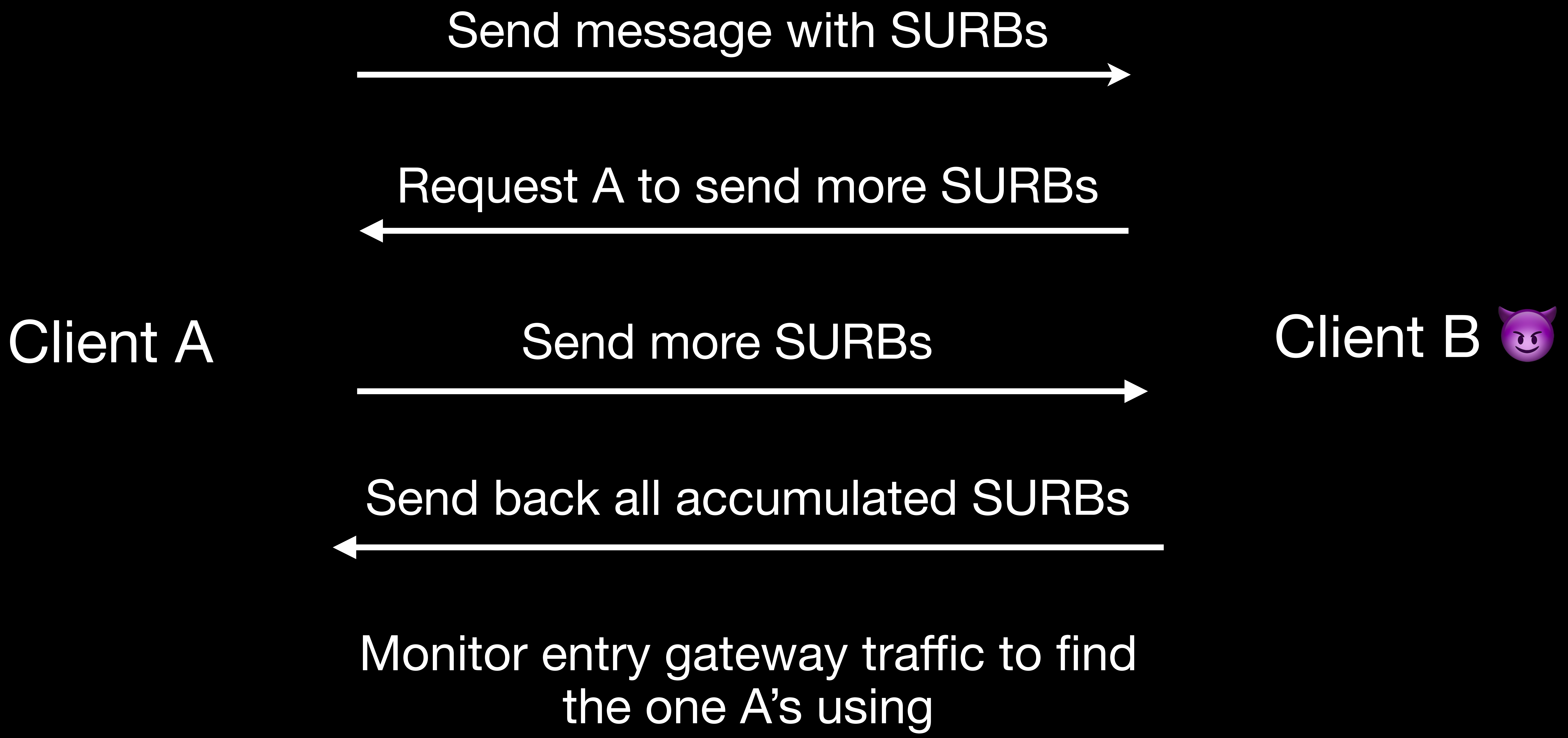
Node 3

Destination

Entry Gateway

Exit Gateway

Anonymous Replies with Single Use Reply Blocks (SURB)



Client A

Client B 😈

Send message with SURBs

Request A to send more SURBs

Send more SURBs

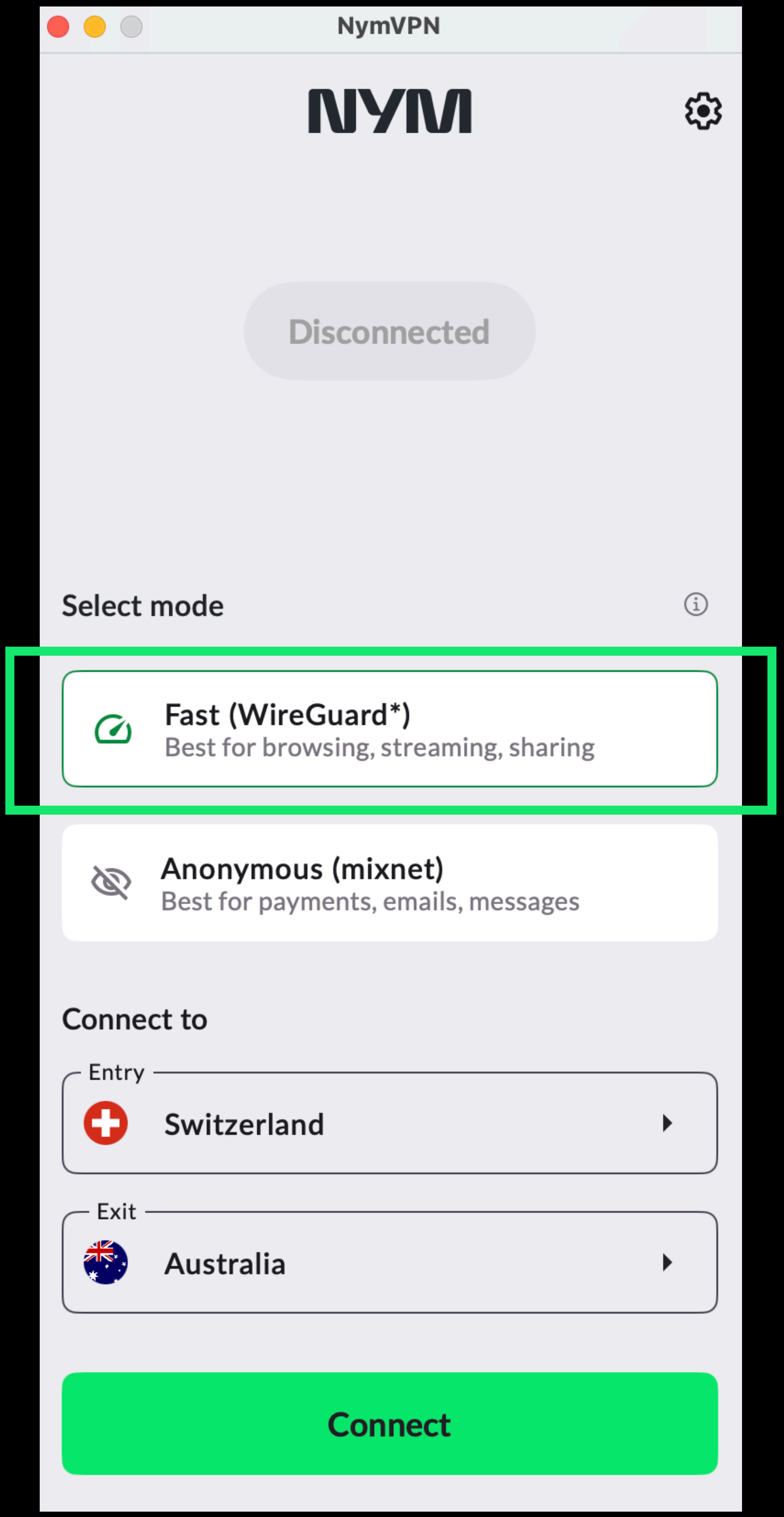
Send back all accumulated SURBs

Monitor entry gateway traffic to find the one A’s using

Verifiable Localization in Decentralized Systems (VerLoc)

Verify nodes are where they say they are without using trusted authorities or landmarks.

Internet roundtrip time between a node and a set of pseudorandomly chosen reference nodes → Distance



NymVPN

NYM

Disconnected

Select mode

Fast (WireGuard*)
Best for browsing, streaming, sharing

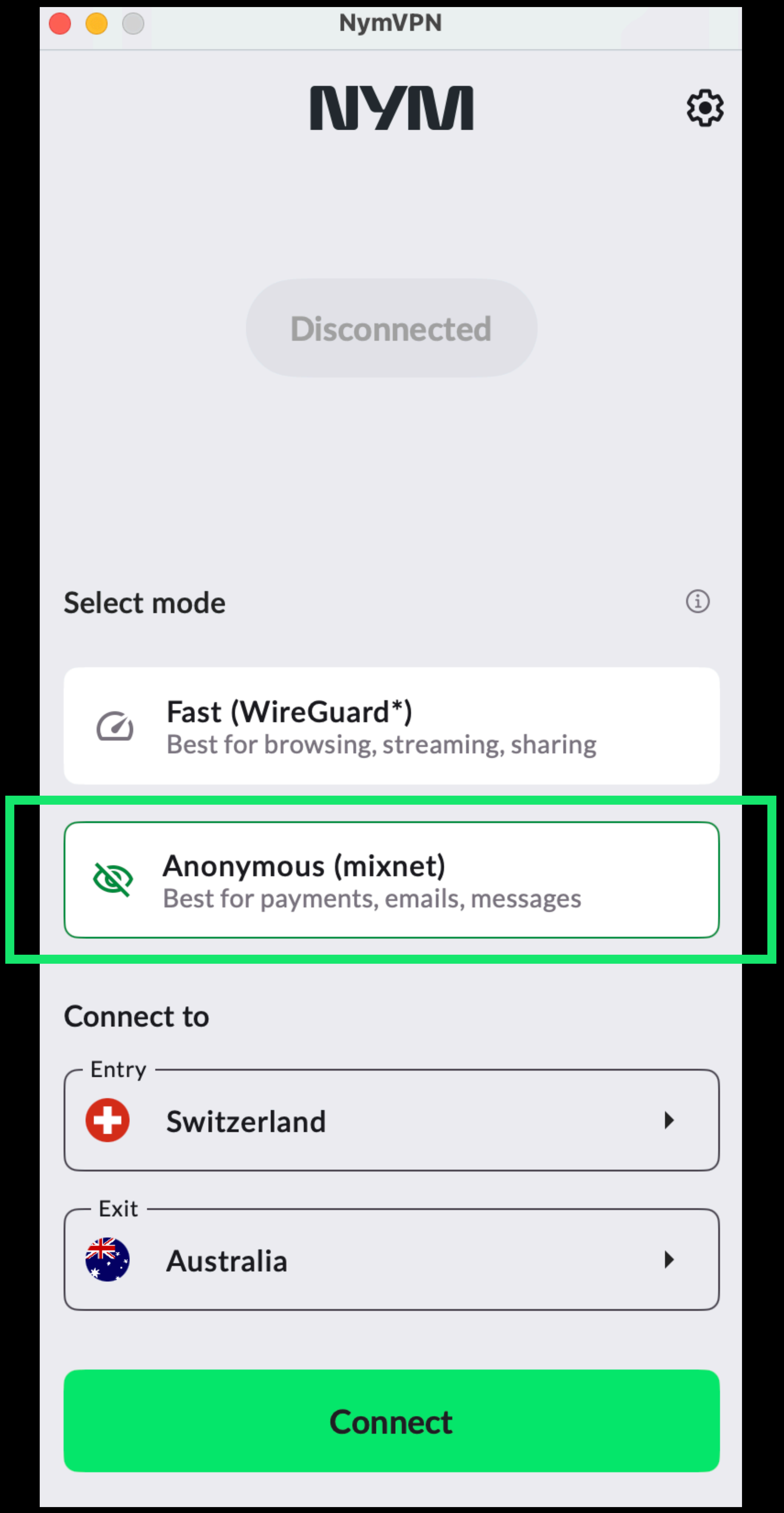
Anonymous (mixnet)
Best for payments, emails, messages

Connect to

Entry
Switzerland

Exit
Australia

Connect



NymVPN

NYM

Disconnected

Select mode

Fast (WireGuard*)
Best for browsing, streaming, sharing

Anonymous (mixnet)
Best for payments, emails, messages

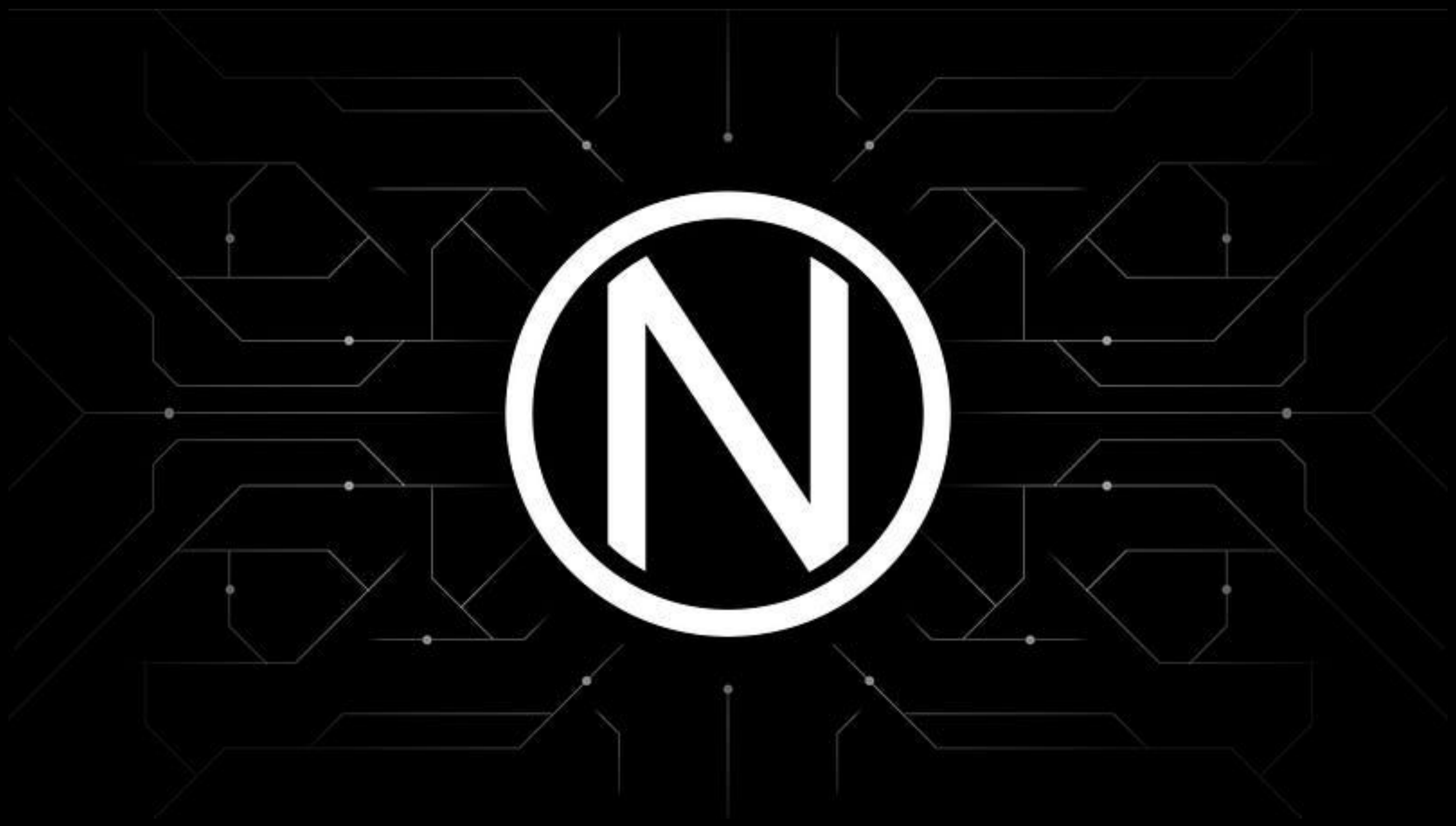
Connect to

Entry
Switzerland

Exit
Australia

Connect

Tokenomics



“Stake”

Node Operators
Delegators

$$\text{active set selection probability} =$$

$$\text{stake} \cdot (\text{config score} \cdot \text{performance score})^{\boxed{20}}$$

LATENCY
ME
makeameme.org

Questions?

@alexiscao.bsky.social