NYM

The Nym Mixnet

Intro to a new anonymous communication network

Speaker

- Jon Häggblad
- Developer
- Mostly Rust these days. C++ and Scientific Computing / Computational Math in a previous life.

The Nym Mixnet

Free Software

- https://github.com/nymtech/nym/
- Apache-2.0
- Mostly written in Rust
- Funded in the past through H2020 PANORAMIX and Next Generation Internet projects on the EU level
- Switzerland based startup that does most of development currently

What is the problem we are trying to solve

Who

- Government surveillance
- Surveillance capitalism

How

- Large scale correlation attacks
    - global passive adversaries with “God’s eye” view of the entire network
- Metadata leaks at the network level

The Nym Platform

“Decentralized incentivised mixnet + private credentials”

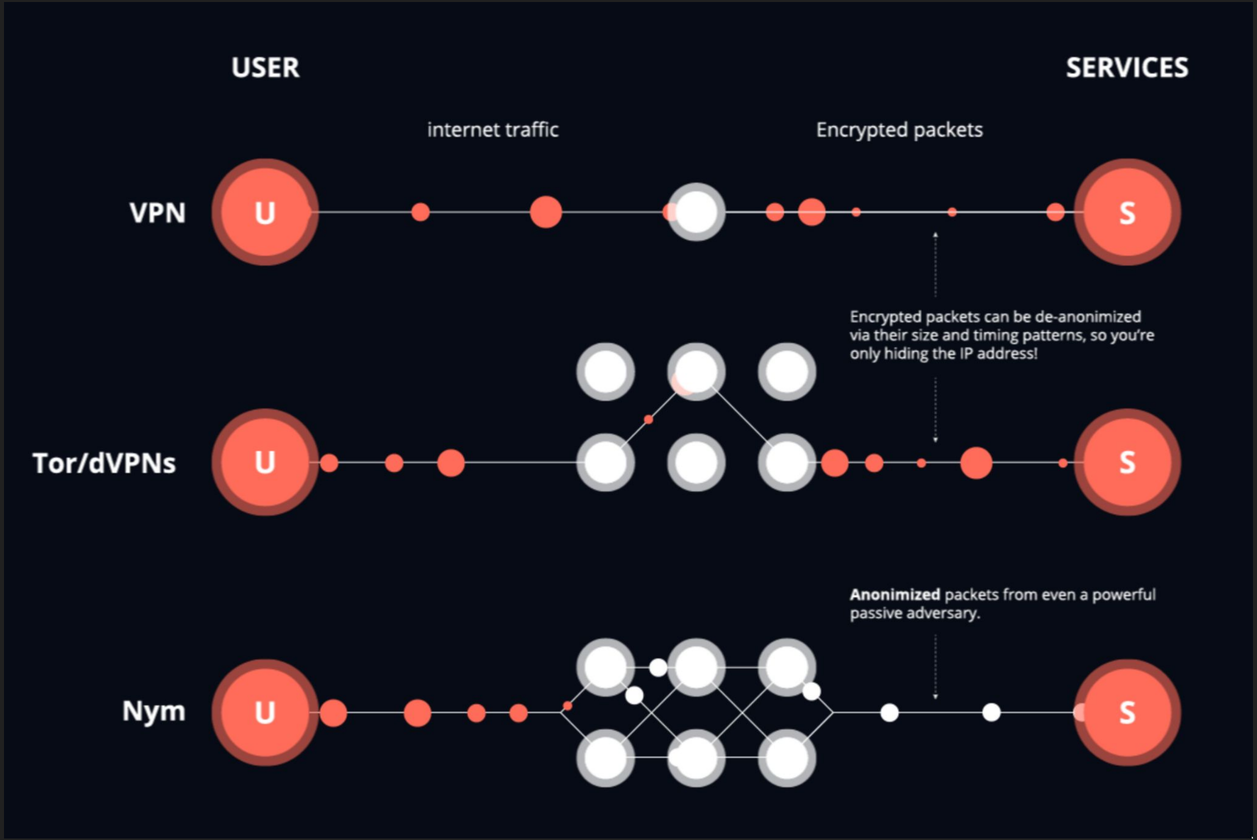
The Nym Mixnet

- Overlay network
- Onion routing
- Based on the Loopix design [1]
- Sphinx packets [2]
- Packet re-ordering and timing obfuscation
- Cover traffic
- Single Use Reply Blocks (SURB)

[1] Piotrowska, Ania & Hayes, Jamie & Elahi, Tariq & Meiser, Sebastian & Danezis, George. (2017).
The Loopix Anonymity System.

[2] Danezis, George & Goldberg, Ian. (2009).
Sphinx: A Compact and Provably Secure Mix Format. IACR Cryptology ePrint Archive. 2008. 269-282. 10.1109/SP.2009.15.

The Nym Mixnet



Encrypted packets can be de-anonimized via their size and timing patterns, so you're only hiding the IP address!

Anonimized packets from even a powerful passive adversary.

Incentivised

- Network directory
  - Set of validators running a consensus protocol
  - Keeps track of all mixnodes and gateways
- Mixnodes are rewarded with NYMs for mixing network traffic
- NYMs can be used to acquire bandwidth credentials (coconut credentials)

Private credentials

Coconut credentials

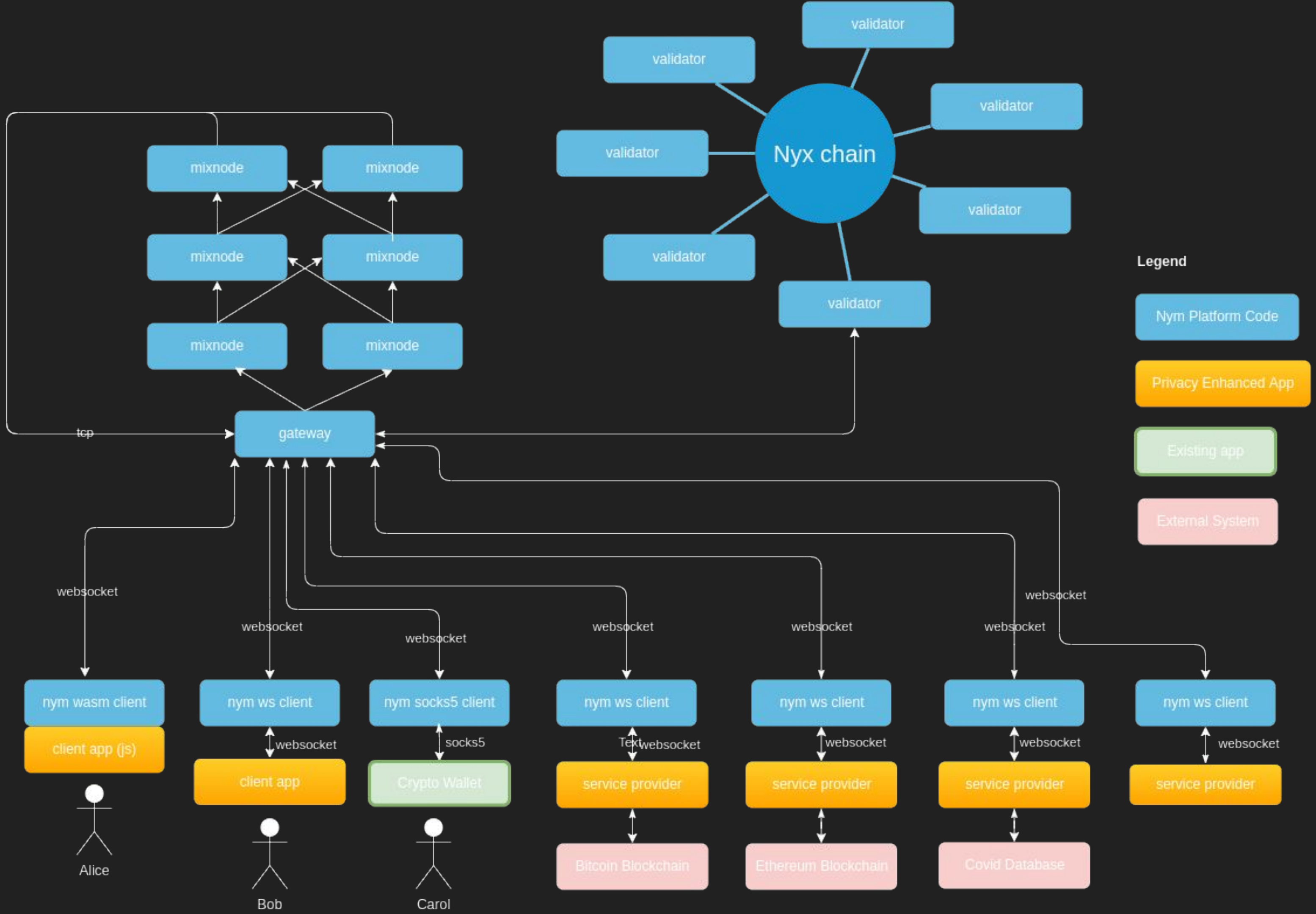
- Break linkability between your identity and your right to use a service

- Re-randomizable
- Blinded
- Selective disclosure
- Decentralized (threshold issuance)

Sonnino, Alberto & Al-Bassam, Mustafa & Bano, Shehar & Danezis, George. (2018). Coconut: Threshold Issuance Selective Disclosure Credentials with Applications to Distributed Ledgers. 10.14722/ndss.2019.23272.

Decentralized

- ~500 mixnodes currently active
- The vision is that this eventually becomes self-running with no need for external funding


validator
validator
validator
validator
Nyx chain
validator
validator
validator
validator
mixnode
mixnode
mixnode
mixnode
mixnode
mixnode
tcp
gateway
websocket
websocket
websocket
websocket
websocket
websocket
websocket
nym wasm client
client app (js)
Alice
nym ws client
websocket
client app
Bob
nym socks5 client
socks5
Crypto Wallet
Carol
nym ws client
Text
websocket
service provider
Bitcoin Blockchain
nym ws client
websocket
service provider
Ethereum Blockchain
nym ws client
websocket
service provider
Covid Database
nym ws client
websocket
service provider
Legend
Nym Platform Code
Privacy Enhanced App
Existing app
External System