The Nym Network: Design and Challenges

Claudia Diaz

Nym Technologies and KU Leuven

Caen, June 24th 2025

Outline

- Goals of the Nym network and practical tradeoffs
- High-level overview of Nym components and NymVPN functionality
  - 5-hop mixnet
  - 2-hop wireguard
  - Anonymous credential system
- Incentive system
- Takeaways and future work

Communication metadata

- **What**: source, destination, time, size, … (not content !)
- **Who**: ISP, IEX, WiFi, eavesdroppers, …
- **When**: every time you are connected online
- **How**: low volume, structured machine language, low legal protection, rich inference value

“Metadata absolutely tells you everything about somebody’s life. If you have enough metadata, you don’t really need content.”

NSA General Counsel Stewart Baker

The Nym wish list: decentralized, self-sustained, general-purpose solution for network privacy

- **Protects** communication **metadata** against network adversaries
- **Usable** by the general public and for a wide range of use cases
  - Latency tolerance, traffic volume and variability, overhead constraints
- **Decentralized** (yet verifiable)
  - All critical functions are decentralized and there are no single points of failure
  - Maintaining ledger of txs, executing smart contracts, issuing and verifying credentials, maintaining network state, …
- Financially **self-sustaining**
  - The network charges for services
  - Income is fairly distributed to the various entities provisioning the service
- **Scalable**

What's achievable in practice: tradeoffs

- Tradeoff between privacy and usability (latency) + overhead (anonymity trilemma)
  - Low-latency constraints + high-variance, large traffic volume: **impossible** to fully protect network metadata towards global network adversaries without extreme overheads ("waste")
  - Latency tolerance + regular or low/moderate traffic volumes: **feasible** to provide high levels of protection for network metadata

What’s achievable in practice: tradeoffs

- Tensions between privacy and decentralization + system integrity
  - Fair and transparent rewards for components (contribution, QoS)
  - Enforcing fair use limits for (anonymous) clients
  - Preventing free riding by adversarial components

What's achievable in practice: tradeoffs

- Tensions between decentralization + privacy and scalability + usability
  - Distribution of node directory
  - Credential verification (including double-spending detection)

- Some components/functions are non-trivial to decentralize
  - Centralized stopgap solutions, eg: payments in non-native currency; network health stats

network privacy

5-hop Mixnet + 2-hop WG

access management: unlinkability + authorization

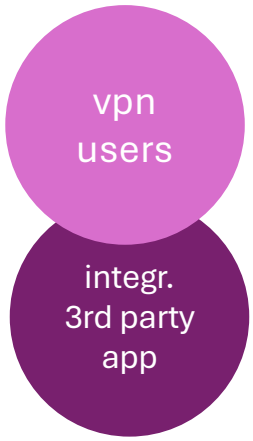
anonymous credential system

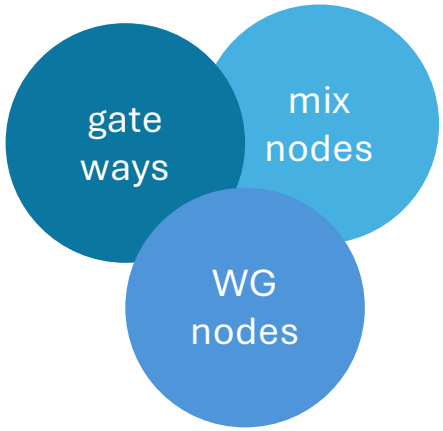
QoS, economic sustainability

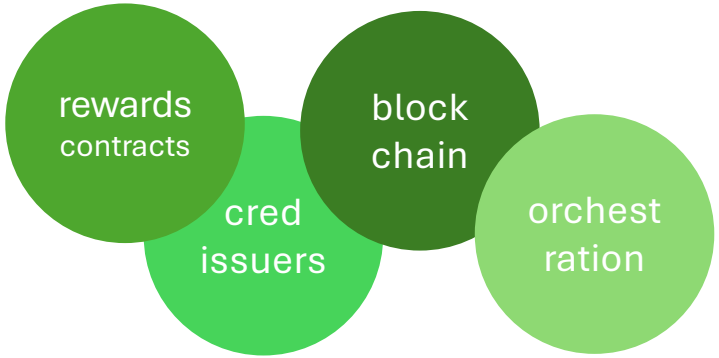
econ system + incentive mechanisms

decentralized orchestration, availability, integrity, verifiability

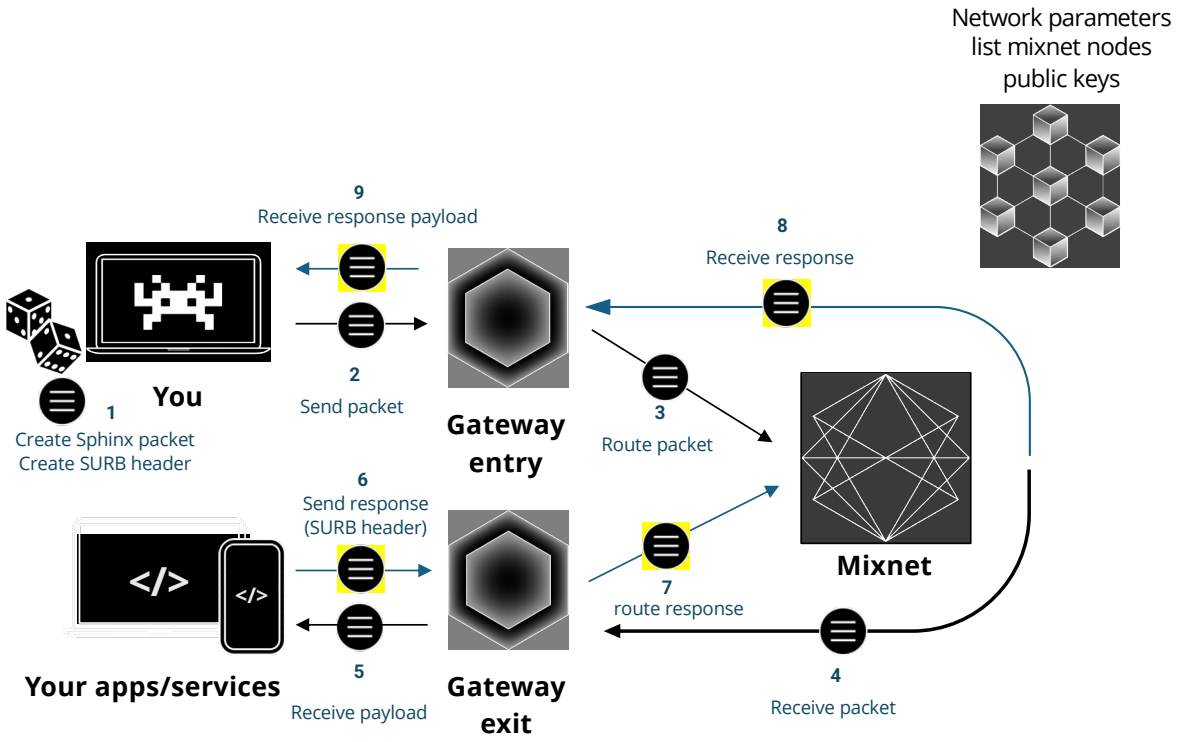
blockchain + temp store







Mixnet component



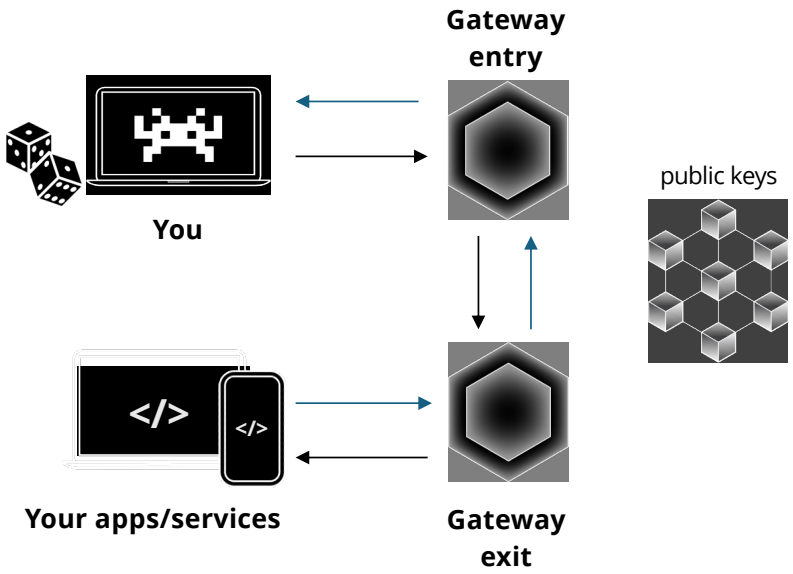
Features

- Packet-based communications
- 5-hop routes (5 layers of encryption + e2e encryption)
- Poisson-regulated sending
- Cover traffic (loop packets)
- Mixing delays (randomized per hop): user-customizable soon
- Anonymous replies via SURBs

Challenges:

- Accurate gateway quantity and quality metrics (reflective of total usage and user experience)
- Poisson sending rates
- Optimal cover traffic strategies
- Free riding prevention/detection
- Exit policies

dVPN (WG) component



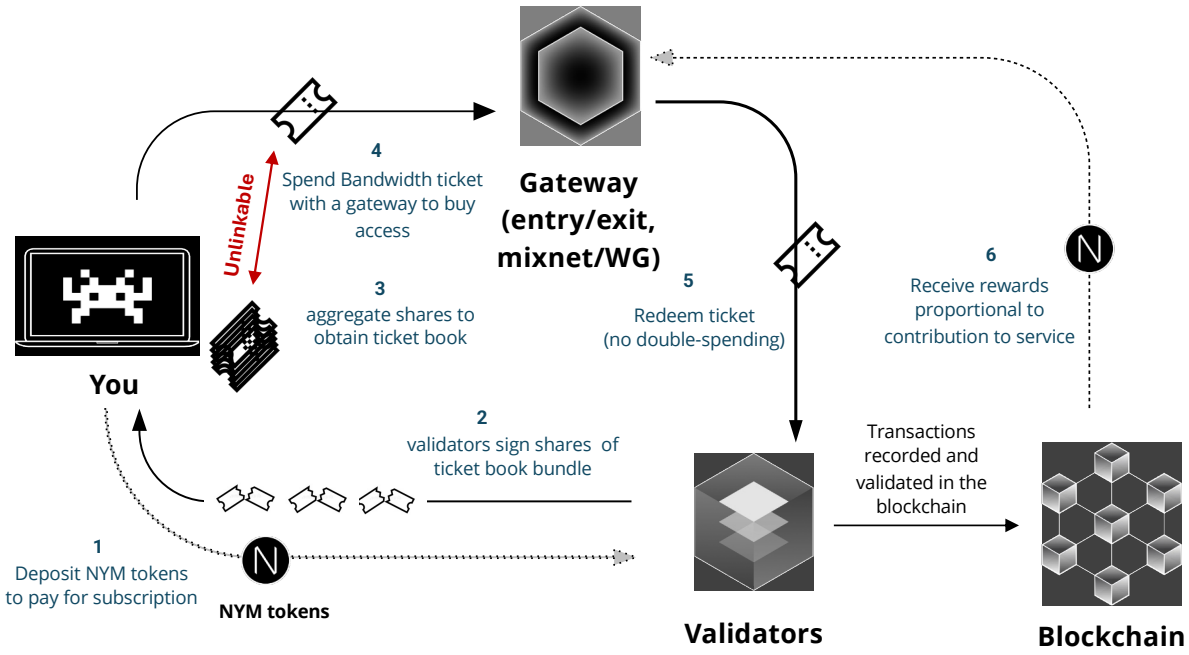
Features

- 2-hop WG tunnel, circuit-based
- No cover traffic or mixing delays
- Suitable for low-latency applications

Challenges:

- Ensuring consistent QoS:
  - gateway stability over time
  - load balancing
  - helping users find suitable gateways (own past experience, shared ratings, current load)
- Independent entry/exit gateway operators:
  - declarations by (honest) operators
  - trust building
  - user interface
- Censorship-resistant access

Anonymous credentials (simplified)



Nym acts as TTP intermediary to enable payments in non-native currency:

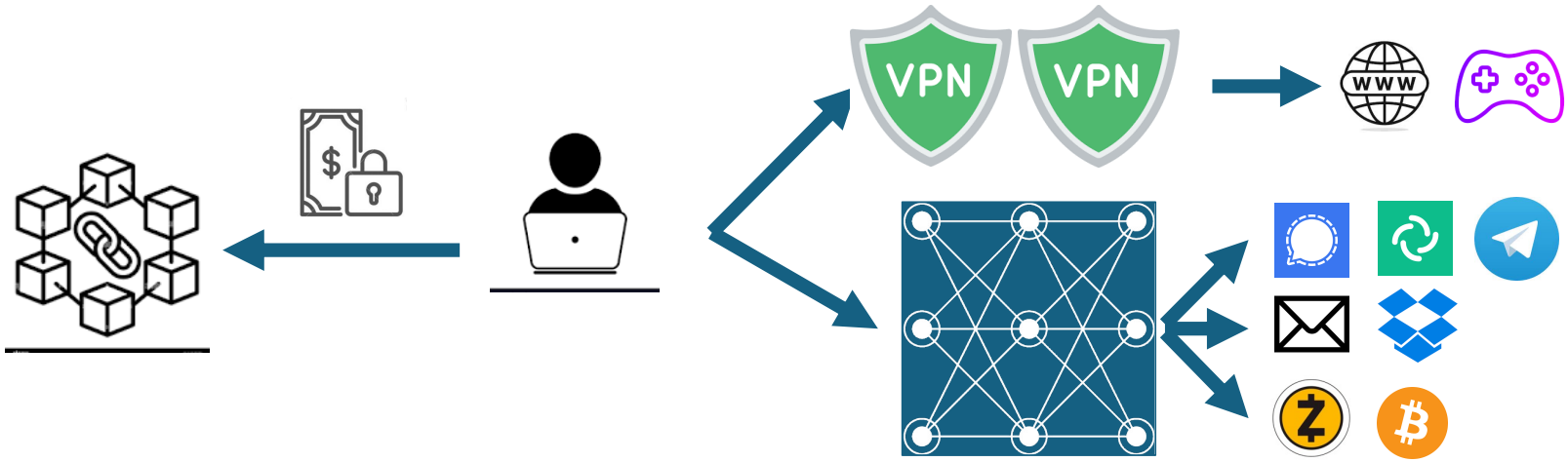
- Buy NYM tokens from the market with fiat/other funds provided by user
- Deposit NYM tokens “on behalf” of user
- User has a public key to prove ownership of subscription

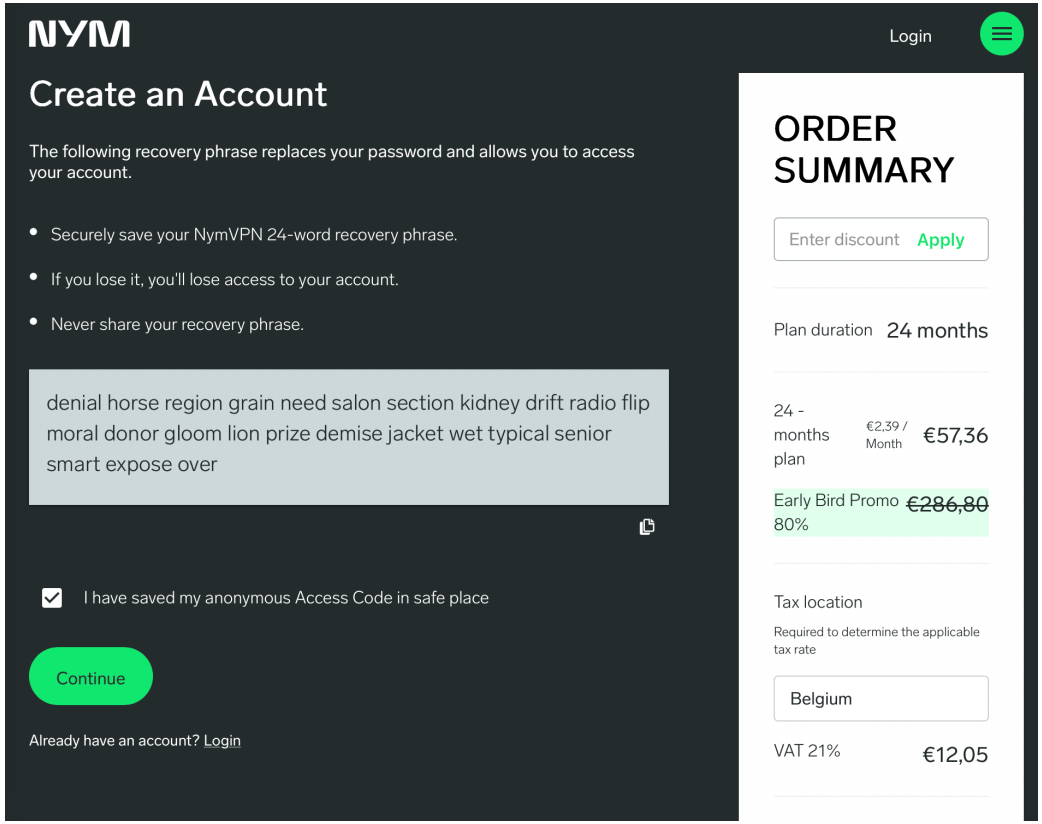
- Features:
  - Decentralized (threshold) issuance
  - Unlinkability of tickets (compact e-cash: wallet=ticketbook, coin=ticket)
  - Double spending protection (combination online/offline)
  - Four ticket types: entry/exit, mixnet/WG

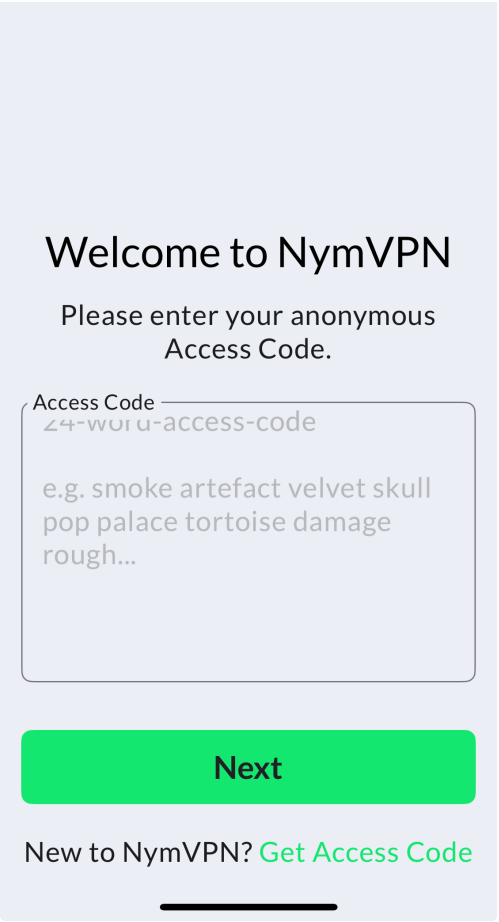
- Challenges:
  - Multiple devices per subscription: distribution of tickets over devices (tension with enforcing fair use limits)
  - Ticket “waste” due to expiration, change of gateway
  - DKG with changes of validator set
  - Validator rewarding based on issued and verified tickets

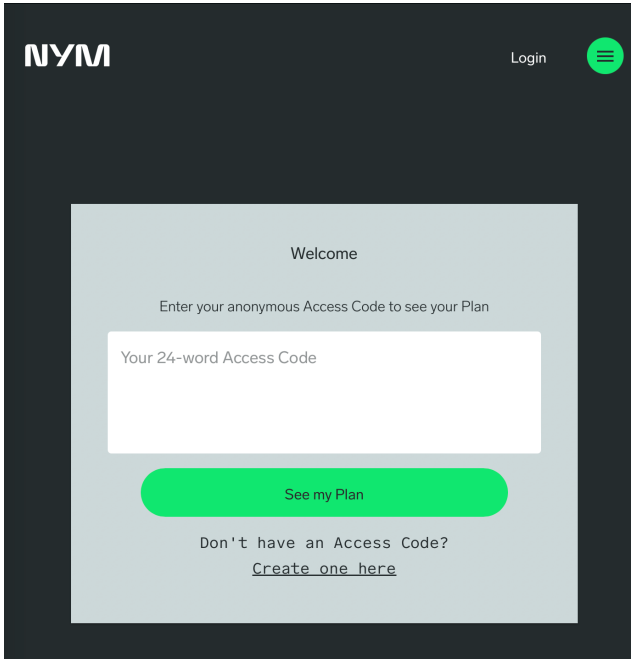
NymVPN

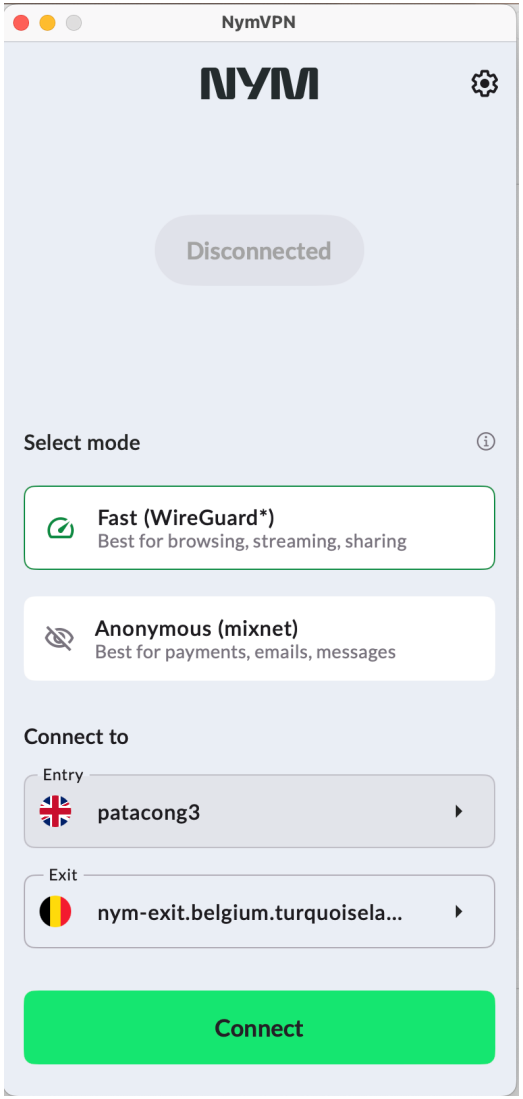
- Commercially viable “vpn-like” service that offers:
  - Private payments that prevent linking activity to identity and profiling
  - A single client app that can use both:
    - 2-hop (“connection-based”) WG tunnels for low-latency applications
    - 5-hop mixnet routes (“packet-based) for latency-tolerant applications

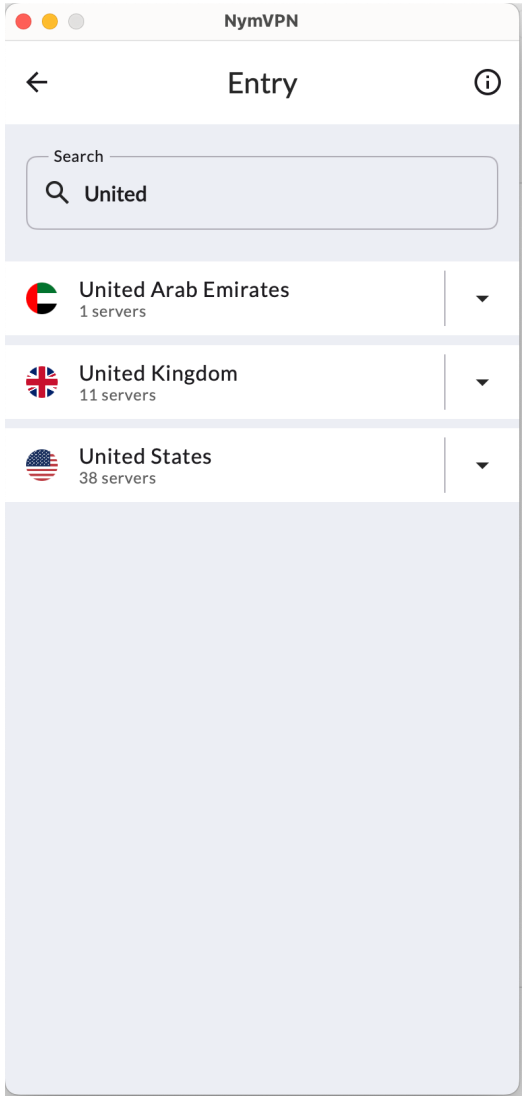


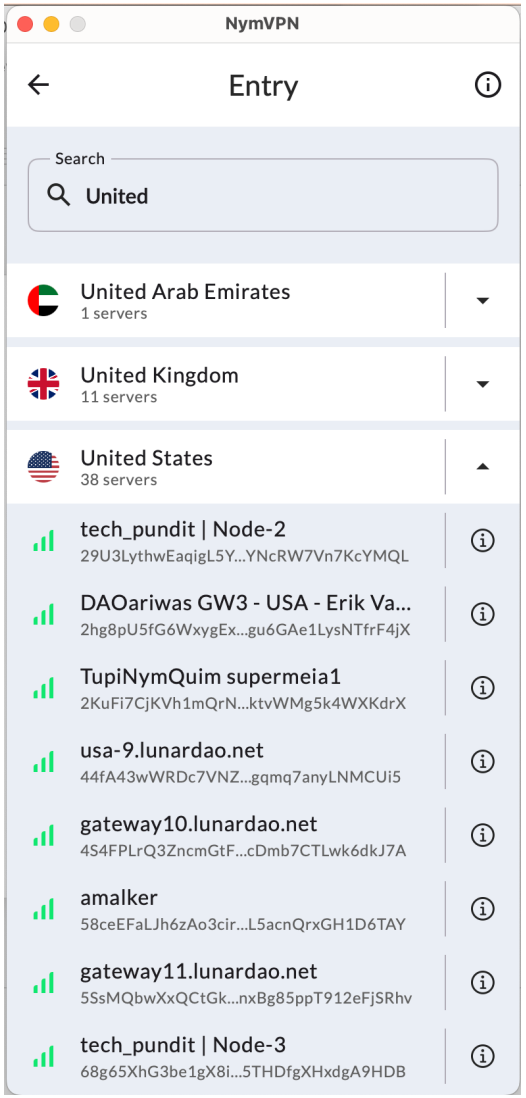

NYM
Login
Create an Account
The following recovery phrase replaces your password and allows you to access your account.
Securely save your NymVPN 24-word recovery phrase.
If you lose it, you'll lose access to your account.
Never share your recovery phrase.
denial horse region grain need salon section kidney drift radio flip moral donor gloom lion prize demise jacket wet typical senior smart expose over
I have saved my anonymous Access Code in safe place
Continue
Already have an account? Login
ORDER SUMMARY
Enter discount
Apply
Plan duration
24 months
24 - months plan
€2,39 / Month
€57,36
Early Bird Promo 80%
€286,80
Tax location
Required to determine the applicable tax rate
Belgium
VAT 21%
€12,05

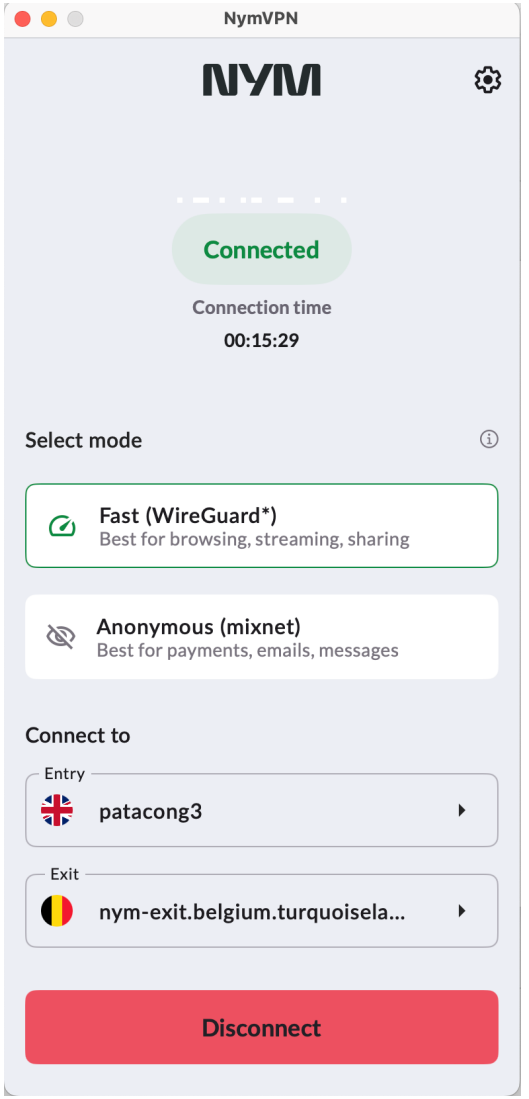

Welcome to NymVPN
Please enter your anonymous Access Code.
Access Code
24-word-access-code
e.g. smoke artefact velvet skull pop palace tortoise damage rough...
Next
New to NymVPN? Get Access Code


NYM
Login
Welcome
Enter your anonymous Access Code to see your Plan
Your 24-word Access Code
See my Plan
Don't have an Access Code?
Create one here

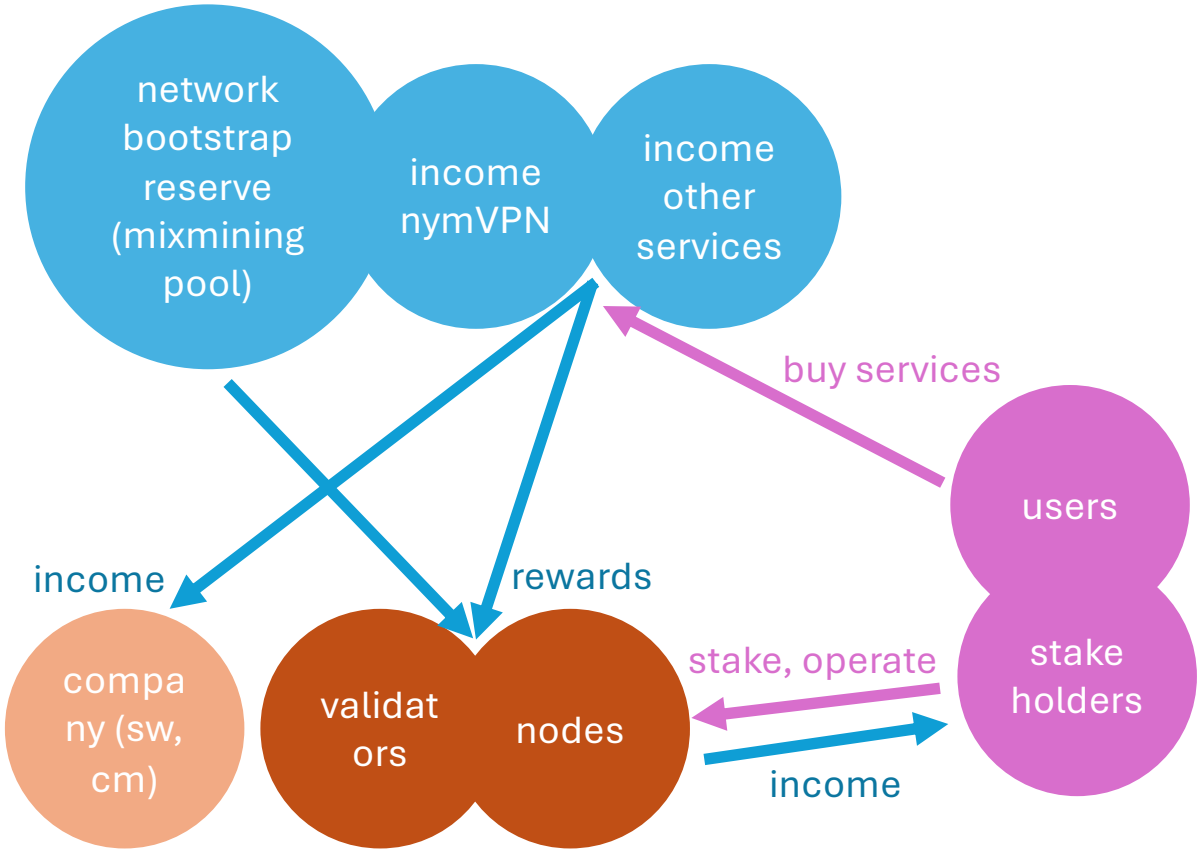

NymVPN
NYM
Disconnected
Select mode
Fast (WireGuard*)
Best for browsing, streaming, sharing
Anonymous (mixnet)
Best for payments, emails, messages
Connect to
Entry
patacong3
Exit
nym-exit.belgium.turquoisela...
Connect


NymVPN
Entry
Search
United
United Arab Emirates
1 servers
United Kingdom
11 servers
United States
38 servers


NymVPN
Entry
Search
United
United Arab Emirates
1 servers
United Kingdom
11 servers
United States
38 servers
tech_pundit | Node-2
29U3LythwEaqigL5Y...YNcRW7Vn7KcYMQL
DAOariwas GW3 - USA - Erik Va...
2hg8pU5fG6WxygEx...gu6GAe1LysNTfrF4jX
TupiNymQuim supermeia1
2KuFi7CjKVh1mQrN...ktvWMg5k4WXKdrX
usa-9.lunardao.net
44fA43wWRDc7VNZ...gqmq7anyLNMCUi5
gateway10.lunardao.net
4S4FPLrQ3ZncmGtF...cDmb7CTLwk6dkJ7A
amalker
58ceEFaLJh6zAo3cir...L5acnQrxGH1D6TAY
gateway11.lunardao.net
5SsMQbwXxQCtGk...nxBg85ppT912eFjSRhv
tech_pundit | Node-3
68g65XhG3be1gX8i...5THDfgXHxdgA9HDB


NymVPN
NYM
Connected
Connection time
00:15:29
Select mode
Fast (WireGuard*)
Best for browsing, streaming, sharing
Anonymous (mixnet)
Best for payments, emails, messages
Connect to
Entry
patacong3
Exit
nym-exit.belgium.turquoisela...
Disconnect

Economic cycle

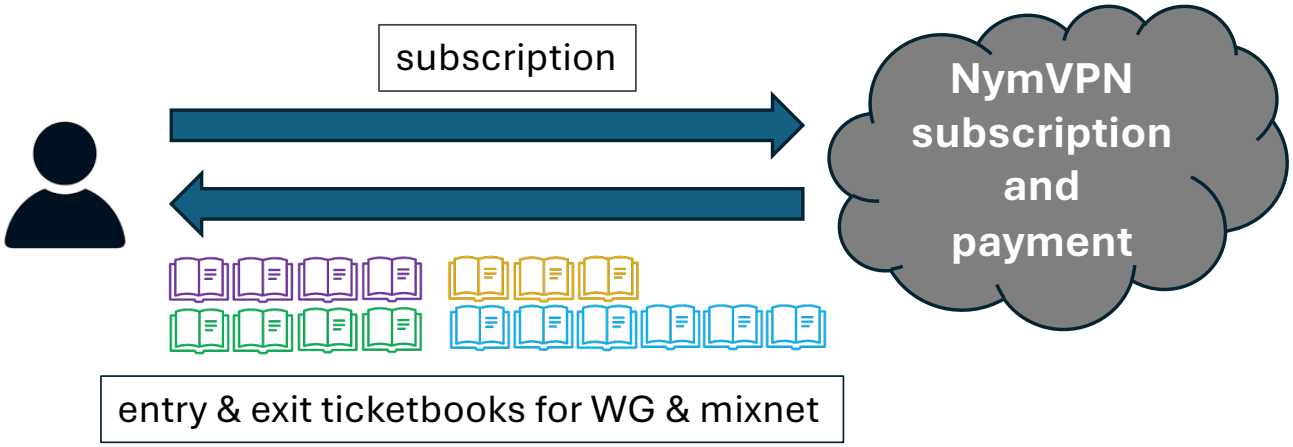


- The native NYM token transfers value within the system from users to service providers
- In steady state, income should fully fund operators + sw dev, cm

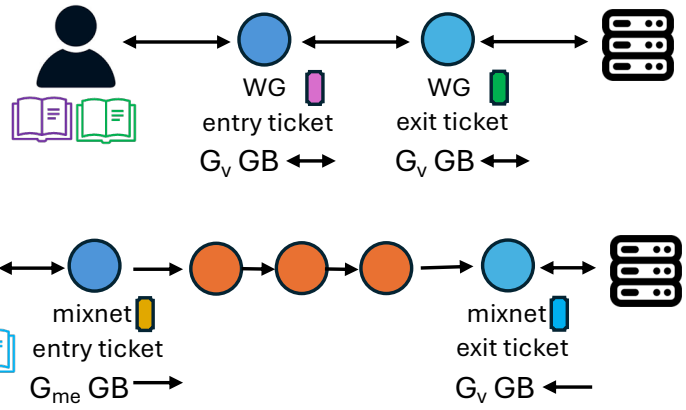
- Challenges:
  - node stake delegation not agile enough to follow performance
  - higher costs of running multi-hop decentralized vpn infrastructure
  - ensuring fair rewarding: no cheating, no free riding
  - embedding the right incentives

Incentive system: goals

- Long-term **viability**: compensate infrastructure operators for their costs and labor; well-performing nodes make a sustainable profit
  - Fairness of rewards: proportional to entities' contribution to the service
- **Scale** the network to meet demand: fund additional operators when user base (and income) grows
- Support **QoS** for client traffic: reward node reliability
- Support **decentralization**: enable a market where many independent operators are competing for rewards by running high-quality nodes
- Support system **integrity**: entities that deviate from the protocols pay an opportunity cost (lost future rewards if expelled)



Fixed number of tickets per ticketbook (50)
Fixed data allowance per ticket type



User obtainins new ticketbooks (until **fair use limit** reached); otherwise → not possible to curb mass sharing of credentials given the privacy properties

Nodes collect tickets from users as proof of the work they have done

Total “work” done by the network (routed GB)

T_{ve}: total nr **vpn entry** tickets spent in the epoch (all nodes)
T_{vx}: total nr **vpn exit** tickets spent in the epoch (all nodes)
T_{me}: total nr **mixnet entry** tickets spent in the epoch (all gateways)
T_{mx}: total nr **mixnet exit** tickets spent in the epoch (all gateways)

$$W_T = \underbrace{(T_{ve} + T_{vx}) * G_v}_{W_{WG}} + \underbrace{5 * (T_{me} * G_{me} + T_{mx} * G_{mx})}_{W_M}$$

W_{WG} (WG GB routed)

W_M (mixnet GB routed)

$s_W = W_{WG} / W_T$: fraction of vpn work in the epoch

$s_M = W_M / W_T$: fraction of mixnet work in the epoch

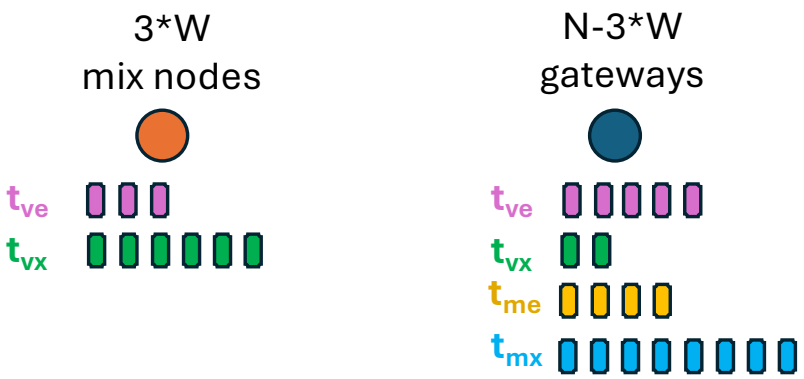
$$s_W + s_M = 1$$

We use the number of tickets of each kind collected by all nodes in the epoch to compute the total work (routed GB) done by all nodes, W_T :

$$W_T = W_{WG} + W_M$$

W_{WG} : GB relayed in WG mode
W_M : GB relayed in mixnet mode

Work contributed by each node / gateway



gateway work:

$$\omega_i = s_W \cdot (0.33 \cdot f_{ve} + 0.67 \cdot f_{vx}) + s_M \cdot (0.16 \cdot f_{me} + 0.36 \cdot f_{mx})$$

mix node work:

$$\omega_i = s_W \cdot (0.33 \cdot f_{ve} + 0.67 \cdot f_{vx}) + s_M \cdot 0.16 \cdot 1/W$$

$$s_W + s_M = 1 \qquad \sum_{i=1}^{N} \omega_i = 1$$

- At the end of each epoch:
  - ALL nodes have collected t_{ve} WG entry tickets and t_{vx} WG exit tickets
  - Mixnet gateways have additionally collected t_{me} mixnet entry tickets and t_{mx} mixnet exit tickets
  - Given all collected tickets (T_{ve} , T_{vx} , T_{me} , T_{mx}) for all nodes, for each node we compute the respective **fraction** of traffic:

$f_{ve} = t_{ve} / T_{ve}$ fraction of WG entry tickets
$f_{vx} = t_{vx} / T_{vx}$ fraction of WG exit tickets

$$\sum_{i=1}^{N} f_{ve} = 1 \qquad \sum_{i=1}^{N} f_{vx} = 1$$

$f_{me} = t_{me} / T_{me}$ fraction mixnet entry tickets
$f_{mx} = t_{mx} / T_{mx}$ fraction mixnet exit tickets

$$\sum_{i=1}^{N-3W} f_{me} = 1 \qquad \sum_{i=1}^{N-3W} f_{mx} = 1$$

W = mixnet layer **width** in the epoch
- Each mix node contributes **1/W** of the layer's work (routes 1/W of all the packets routed in the layer)

Layer weights (**exit premium**, voted by community):
- **33/67** for (2-hop) WG
- **16/16/16/16/36** for (5-hop) mixnet

Node rewards (mix nodes, gateways, wireguard)

Rewards $\boldsymbol{R_i}$ for node $\boldsymbol{i}$:

$$\boldsymbol{R_i = R \cdot \rho_i \cdot \sigma'_i \cdot (\omega_i + \alpha \cdot \lambda'_i) \cdot \frac{1}{1+\alpha}}$$

- $\boldsymbol{R}$ = total mixmining rewards available for all nodes in the epoch
- $\boldsymbol{\rho_i} = 1$ when the node is reliable
  - Otherwise: % of reliability
- $\boldsymbol{\sigma'_i} = 1$ when the node is fully saturated (stake)
  - Otherwise: % of stake saturation
- $\boldsymbol{\omega_i}$ is the **work** contribution of the node
  - Computed based on tickets and mixnet width
- $\boldsymbol{\alpha} = 0.3$ is constant (premium high bond)
- $\boldsymbol{\lambda_i'}$ = node bond (capped at saturation level) divided by staking supply
  - note: λ'_i is a usually a small number
- Leftover rewards remain in the reserve (pool)

Decentralized measurements: concept

- Currently: “network monitor” probe sends packets through random mixnet routes back to itself
  - Infer which nodes are responsible for dropping packets that do not arrive
- Decentralized proposal:
  - “Secret shoppers” approach where some (lottery-based) of the packets sent by clients are indistinguishable and unforgeable “measurement packets”
  - Nodes commit to which packets they have routed in a time period
  - “Measurement packets” are revealed as such after the node commitments
  - Based on measurement openings, everyone can :
    - Reconstruct the measurement packets with their routes and per-mix identifiers
    - Verify whether the mix nodes in the packet path reported the measurement
    - Derive performace scores for all mix nodes

Future directions

- Integrations with other applications (beyond NymVPN)
- Censorship circumvention
- Post-quantum cryptography
- Secure enclaves, trusted execution
- Replacing some (or all !!) of validators' functions (blockchain, temp storage, credential issuing, contract execution) by 3rd party services

Takeaway points

- Nym's goal is to be a network privacy solution that is usable by the general population, decentralized, financially self-sustainable, and scalable
- In practice, it's hard to fully achieve all the previous properties so tradeoffs and compromises are inevitable
- Nym integrates multiple components and technologies:
  - Nodes that route traffic in a 5-hop mixnet and a 2-hop wireguard
  - Anonymous credential system that allows for private payments and access
  - Incentive mechanism to encourage participation and cover operational costs
  - A blockchain to orchestrate components, maintain state, ensure integrity of rewards
- Nym has launched a commercial vpn product "NymVPN"
- Open questions wrt applied research and engineering