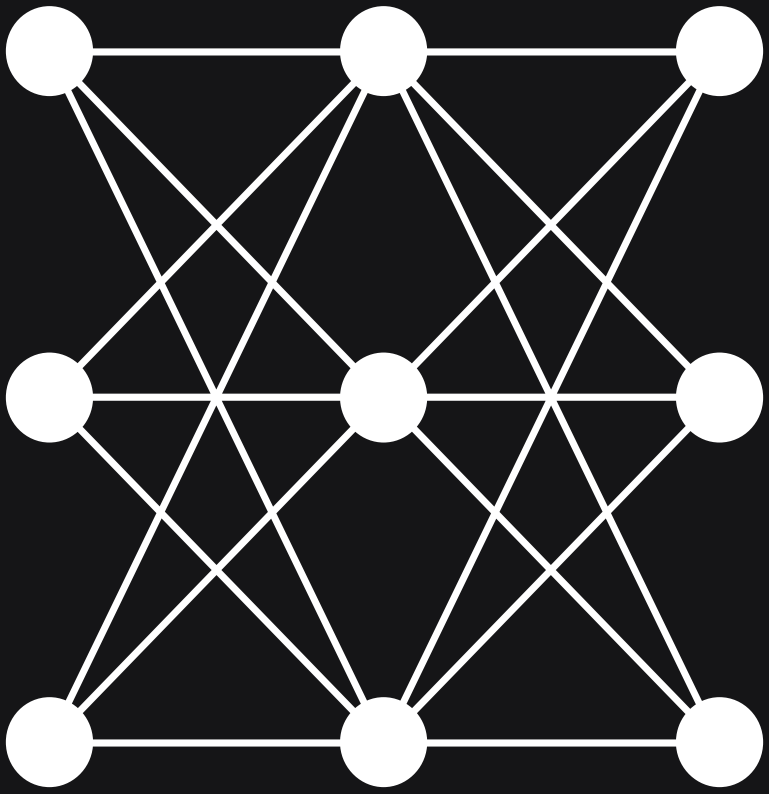
The next generation of Privacy infrastructure



NYM

nymtech.net

The next generation of privacy infrastructure

The Nym network is a decentralized and tokenized infrastructure providing holistic privacy from the network layer to the application layer.

With Nym, you can communicate freely without censorship or fear. Combining a decentralized mixnet and a credential system, Nym weaves token-based incentives into the ecosystem it enables, delivering privacy that is both sustainable and scalable. Nym fills in the missing pieces of the cryptographic revolution necessary to end mass surveillance.

INDEX

1

Surveillance: a stranglehold on the future

The internet is the collective mind of humanity, The circulatory system of thought itself.

Those who control the internet control the future of our species. In a time when authoritarian regimes are resurgent around the world, the risks of centralizing the internet in a handful of institutions are obvious. Privacy is a fundamental aspect of freedom: the ability to communicate and co-create our lives without interference from third parties. If we can't control our data, we can't control our lives.

Today, data about every intimate aspect of our lives is concentrated in the hands of a few corporations. Government agencies harvest it without our knowledge or permission. This is destroying trust in the internet, stifling innovation, and exposing millions to privacy breaches and identity theft.

Existing end-to-end encryption models can protect the content of your communications data—but they do not protect the metadata about whom you are communicating with and when. As Edward Snowden confirmed, the National Security Agency (NSA) has been collecting metadata on a massive scale, indiscriminately spying on the entire internet. No current system can protect you against traffic analysis at scale.

Nym protects both content and metadata, keeping the relationship unlinkable between client devices at one end and service transactions at the other. Nym's fundamental innovation is a holistic, open-source, decentralized, permissionless, and incentivized network: a secure foundation on which developers can build applications that can anonymize metadata both at the level of network traffic and at the level of applications. Nym is designed to transmit data without access to or knowledge of the source, location or content of that data by the network or its participants.

At the heart of the Nym network is the NYM token. The NYM token decentralizes the system via proof-of-stake; it can enable the functioning of the system via distributing rewards in exchange for provisioning privacy-enhanced communication. Tokenization provides the foundation for an alternative to the surveillance-based economic models thatdominate today's internet.

2

How Nym works

Privacy is a property of an entire system taken as a whole, not any one aspect of the system.

Even if you use the most advanced cryptographic tools to secure one layer of your communication, it won't be private if the other layers leak information.
Nym's goal is to provide privacy to all internet traffic across multiple layers by deploying a generic system that can scale by design to include the entire world.

Nym is comprised of two components:

1. **A decentralized mixnet that protects users' network traffic (layer 0), improving on the models represented by VPNs and Tor.**

2. **A tokenized credential system that provides application-level privacy and that enables users to access the Nym mixnet.**

A tokenized credential system that provides application-level privacy and that enables users to access the Nym mixnet.
We do not believe it is feasible for the communication system we envision to operate for free, on a fully volunteer basis. Economic incentives are necessary to encourage participation and to avoid network abuse. To that end, the network requires users to utilize NYM tokens. These tokens are used to pay for and are integral to the provisionof network services.

For example, mixes are rewarded for mixing (the intensive but useful computation needed to route packets on behalf of other users in a privacy enhanced manner)rather than mining. Designed to be compatible with any blockchain, a Nym blockchain maintains the state of credentials and the operations of the mixnet so the Nym network can be decentralized, permissionless, and trustless. Use of the token also prevents network abuse and an economic disincentive to "spam" the system.

Nym provides stronger privacy than any single-use-case mixnet or isolated application of privacy-enhancing technologies or cryptographic primitives. Because its infrastructure supports so many different applications, Nym can blend large, diverse user bases of different applications into a single massive crowd. This is a breakthrough, because in order to be anonymous when using a system, you must be indistinguishable among a group of users—and the larger the group, the better the privacy.

3

The NYM token

Privacy is priceless.

It is the difference between a society based on top-down control, and a society based on freedom. In the mass surveillance machine that Google and Facebook have created, privacy is given a value of zero. Market forces have failed to identify how important privacy is. The NYM token gives users a way to affirm the value of privacy by participating in collectively building the infrastructure that secures it and paying for the provision of network services that the infrastructure provides.

Nym tokens provide credentialed access to privacy-enhanced and uncensored internet communication for a unit of time. The NYM token is a voucher for these credentials and is used to pay for network operations. For example, tokens will be used to reward those who provide services for the Nym network,such as operating a mix-node or validators for the Nym blockchain.

Tokens will be used to reward those who put stake into the Nym ecosystem by providing services, such as operating a mixnode or validators for the Nym blockchain.

As we want to reward those who provide valuable mix-nodes and validators early on, NYM tokens have a deflationary reward schedule.

Staking is an integral component of the provision of network services. It ensures that all the participants in the Nym network—the mix-nodes that compose the mixnet, the validators that maintain the chain, and the service providers that allow users to access their services via that mixnet—are incentivized to give users the highest quality of service via “mix-mining” rewards. Like Bitcoin, the Nym network makes it possible to take fees on transactions; as more apps and users join the Nym network, fees will overtake mix-mining rewards as the primary source of income for the operators of mix-nodes, mix guards and Nym validators.

4

The Nym Architecture

Components

Users want to access service providers securely and privately.

Users run client software (“clients”) that is compatible with the Nym network. The client software allow users to create credentials and thereafter send of packets into the Nym mixnet.

1. **Validators**
   distribute partial credentials to users, produce blocks in the Nym blockchain, measure mix-mining rewards, and maintain synchronization with other blockchains that require privacy.

2. **Mixnet**
   a network of mix-nodes that “mixes” packets to ensure network-level privacy.

3. **Mix guards**
   check whether clients have a valid Nym credential to use the mixnet and provide resistance against denial-of-service attacks and censorship.

4. **Mix-nodes**
   receive mixnet data packets hat they process cryptographically using the Sphinx packet format) and retain for a random amount of time before forwarding those packets on to the next hop in the mixnet.

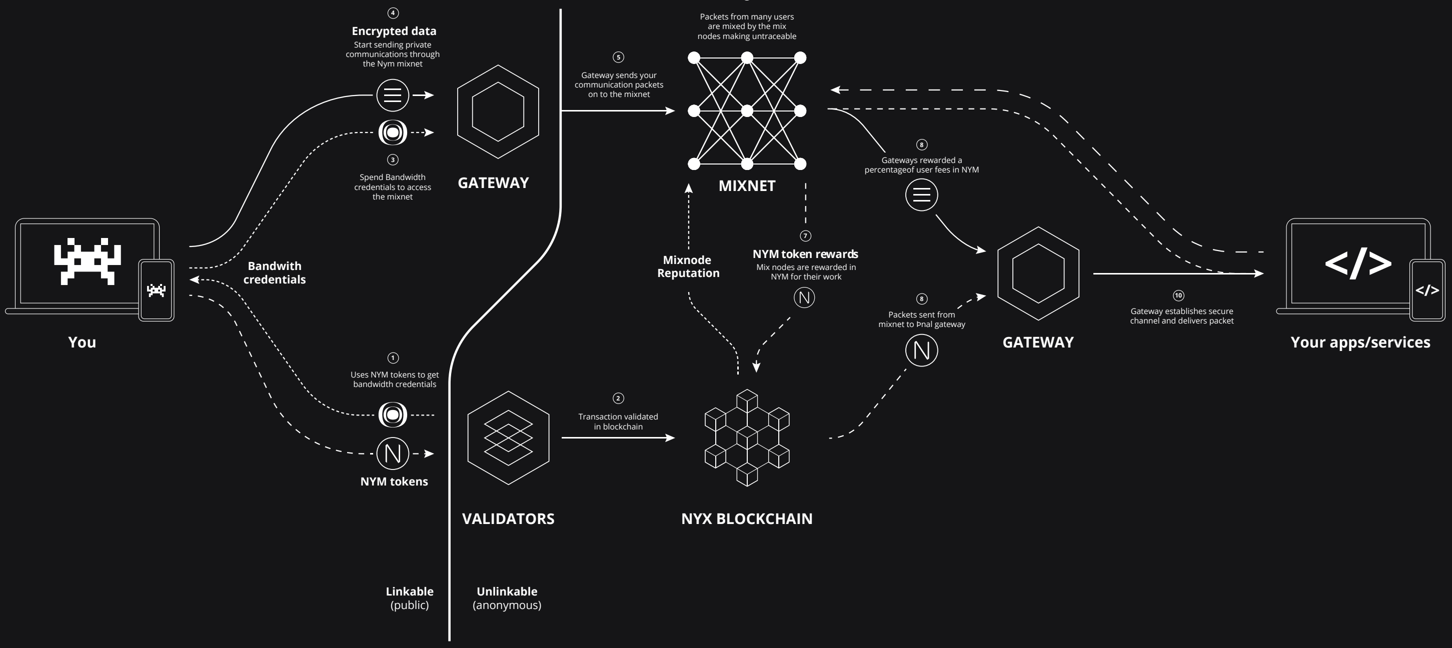
5. **Service Providers**
   receive mixnet data packets hat they process cryptographically using the Sphinx packet format) and retain for a random amount of time before forwarding those packets on to the next hop in the mixnet.

6. **Nym Blockchain**
   is maintained by validators that, for each period of time, maintain the data needed by the Nym network, from the public keys and topology of the mixnet and validators.

7. **External Blockchain**
   blockchains like the Ethereum blockchain that support wallets that can hold the NYM token or the Bitcoin blockchain , where their native cryptocurrency can be converted into NYM tokens.

8. **Identity Providers**
   third parties that can verify, upon user request, attributes that are encoded in the Nym credentials.

Information flow


4
Encrypted data
Start sending private communications through the Nym mixnet
3
Spend Bandwidth credentials to access the mixnet
GATEWAY
You
Bandwith credentials
1
Uses NYM tokens to get bandwidth credentials
NYM tokens
VALIDATORS
Linkable (public)
Unlinkable (anonymous)
5
Gateway sends your communication packets on to the mixnet
6
Packets from many users are mixed by the mix nodes making untraceable
MIXNET
2
Transaction validated in blockchain
NYX BLOCKCHAIN
Mixnode Reputation
7
NYM token rewards
Mix nodes are rewarded in NYM for their work
8
Gateways rewarded a percentageof user fees in NYM
8
Packets sent from mixnet to Þnal gateway
GATEWAY
10
Gateway establishes secure channel and delivers packet
Your apps/services
</>

When a user wants to access a service using the Nym mixnet to make their transactions private against even the most powerful adversary:

Users run client software ("clients") that is compatible with the Nym network. The client software allow users to create credentials and thereafter send of packets into the Nym mixnet.

1. **Users discover service providers and attributes a service provider needs.**
   Users may pay service providers outside of Nym directly. Alternatively, users may pay the mixnet fees directly or services may pay for or stake NYM tokens on behalf of a pool of users in order to provide services without cost to users. A small fraction of payment for service providers can be taken as a fee to reward validators and mix nodes.

2. **Users gather attributes that a service provider needs.**

   For example, the service provider may need proof of age or nationality. If the service requires verification of the user beyond what a user self-certifies, the user can choose to obtain certified attributes from external identity providers ranging from government-verified identity to a web of trust between friends.

3. **Users receive partial credentials from validators:**

   The user's software provides encrypted attributes to validators. The validators then issue signed partial credentials to users.

   Users create credentials locally. A user's software client aggregates the signed partial credential given by validators into a credential needed by the service provider and mixnet guards. Users make credentials anonymous. The user's software client re-randomizes the user's credentials so that credentials are unlinkable to their original signing and issuing, preventing deanonymization of the credentials.

4. **Users show credentials to connect to mixnet guards.**

   Guards forward the clients' traffic to the mixnet while defending against denial of service attacks and checking bandwidth constraints.

   Users send credentials to service provider via mixnet. The first message should contain the credential with any information the service provider needs to initialize a new account or continue usage of old one. The user sends the rest of the messages with application-specific data.

   Users send messages through the mixnet Application-specific data goes to the service provider of their choice. All messages sent over mixnet are unlinkable to the sender due to the mixnet providing delays and cover traffic. Users may receive unlinkable responses via the use of SURBS (Single-Use Reply Blocks).

5. **The service provider records credential usage on Nym blockchain.**

   This prevents double-spending of credentials. If the credential is double-spent, the service provider may deny service to the user.

6. **Rewards are given out by the Nym network to participants based on the mix-mining algorithm.**

   If the service requires payment, the service provider receives payment taken for their services. Fees are taken out to reward the Nym network.

Mix-mining rewards

Nym develops on both proof-of-work and proof-of-stake designs to create a proof-of mixing system called "mix-mining." Where proof-of-work incentivizes solving arbitrary hash puzzles, mix-mining rewards mixnodes for doing computation for privacy.

Mix-mining combines the best aspects of both proof-of-work (cryptographic proof that a mix-node and validator has acted correctly) and proof-of-stake (mix-nodes and validators place a stake in NYM tokens that can be slashed if they misbehave, while users can delegate stake to the mix-nodes and validators of their choice). Mix-nodes earn mix-mining rewards in the form of new NYM tokens, as well as possibly fees from service providers and users of the mixnet.

Mix-nodes are rewarded via the usage of a Verifiable Random Function (VRF) to select verifiable random paths through the network; then traffic is sent through the network via these paths. If this special measurement traffic is not dropped, as can be proven via commitments, then the mix-nodes are rewarded for honestly mixing user traffic.

Validators, and service providers are rewarded by presenting verifiable proofs of how many credentials they processed. The network distributes rewards every time period and updates the mixnet and set of validators to prioritize those with a track record of high quality of service, such as uptime and throughput.

The use of the NYM token for staking to enter the network and slashing when quality of service is not met ensures that every part of the network is disincentivized from malicious and poor performance, while rewards attract those who can meet quality requirements.

5

How does Nym compare to other systems?

Today, external parties can monitor your traffic in order to determine what services you're accessing, who you're communicating with, and when you are doing so.

Even if you use an encrypted messaging service like Whatsapp, Telegram, or Signal, it is possible to determine who you are messaging and when. This is the problem of layer-zero privacy, or privacy at the network level.

Cryptocurrencies such as ZCash, Monero, and Mimblewimble may achieve privacy on the blockchain level but can be deanonymized by timing and associated metadata on the network level. This is true of any zero-knowledge proof system used in isolation on a single level.

VPNs appear to solve this problem but force the user to trust the VPN provider with their data, and the privacy they offer can be broken by adversaries that can observe the entry and exit points of the VPN. Tor and I2P provide a more sophisticated multi-hop solution, but cannot provide strong privacy guarantees against a powerful adversary that can observe the entire network—or just its entry and exit points, as it is not anonymous towards end-to-end network adversaries. Unlike Nym, Tor is optimized for low-latency web browsing and so does not mix packets or generate cover traffic.

Why mixnets?

A mixnet provides multiple hops like Tor but adds timing obfuscation via random delays and cover traffic so a powerful external observer cannot identify a user based on the patterns of their network traffic. Like Lightning, our mixnet uses the Sphinx packet format to make all messages the same length and bitwise unlinkable. The amount of time a packet is delayed is chosen from a probability distribution that can be matched to provide the latency needed for a given use-case. In addition, the Nym mixnet provides a powerful set of usability and performance features other mixnets lack. The Nym mixnet ensures that messages are received and can be re-sent as needed, and that messages are received within a time frame users find acceptable; SURBs allow bidirectional anonymous communication over the mixnet.

In the early 2000s, when Tor was being built, the internet was too slow to allow mixnets to function at an acceptable speed for everyday usage. Today, increased speed, along with a modern mixnet design developed by the team behind Nym, have rendered it possible to develop mix-networking fast enough for regular users, and without scaling limits. One of the advantages of the Nym network is that rather than slowing down with more users, the system can become faster and more private as the anonymity set grows.

Why nym credentials?

Would a powerful general-purpose anonymous overlay network like the Nym mixnet run out of capacity and be abused? Adam Back originally invented Hashcash to prevent email spam and denial of service attacks from being anonymized using the mixnets of that time, like Mixmaster; it is now used in proof-of-work systems. Nym uses cryptographically anonymous credentials to prevent these kinds of attacks, while also enabling the authentication and authorization of users in a way that doesn't leak personal data to external adversaries, as well as to service providers via selective disclosure of attributes.

Nym credentials serve as a privacy-enhanced and decentralized alternative to OAuth-based systems like Facebook Login and Google Sign-In, while sharing even less data on-chain than W3C DIDs. In effect, Nym credentials allow users to selectively disclose their data to whomever they choose, however they wish to, backed up by the power of cryptography and decentralization. Combined with mixnets, Nym provides a holistic solution to privacy that can be integrated with any blockchain and any other application.

6

The door to a new world of innovation

Nym enables service providers to integrate into our network with minimal changes to their code, making it easy to add privacy to existing applications.

As a network that runs on top of the existing internet, the impact of Nym will be tremendous. The potential worth of this ecosystem could be comparable to the value created by the introduction of widespread encryption in the 1990s in the wake of the "crypto wars."

For developers, the questions are: What sort of applications could I build if I could enable strong privacy for my users? What new applications could I create if I could receive fair payment for providing these applications without being dependent on Google Play or Apple's App Store?

Nym enables you to build your application knowing that you can keep the data private. The Nym ecosystem can integrate a diverse range of applications, including private messaging services resistantto traffic analysis, privacy for distributed VPNs, anonymous broadcast of transactions to blockchains, privacy-enhanced file sharing, and single sign-on authentication services without losing control of personal data.

We already have interest from partners seeking to break ground on many fronts— from enhancing the privacy of the Lightning Network, to secure messaging via Status. Additional partners will be eager to work with Nym—from nation-states and enterprises that seek to protect their communication against state-level surveillance to individuals who wish to guarantee their freedom of communication. If you want to partner with us, get in touch.

7

Remember, Remember the 5th of November

When people can speak freely among themselves, it is impossible to oppress them.

Effective privacy tools for the individual mean freedom for society. If not for the ability to communicate on our own terms without censorship and surveillance, we would still be living under hereditary kings.

Today, humanity is facing unprecedented crises—from the destruction of the natural world to the proliferation of new technologies of surveillance and repression. It is more important than ever that we are able to innovate and exchange freely; our survival depends on it.

You can end pervasive surveillance. You can support Nym-enabled services, using your own computer as a mix-node or delegating your stake to others who help run the Nym infrastructure. With your participation, Nym will level the playing field between top-heavy institutions of today and the innovators of tomorrow, enabling us to free ourselves from tyranny via the power of cryptography.

Every technological breakthrough like this has been followed by revolutions that transform society. If the previous generation of encryption technologies paved the way for Tor and Bitcoin, think what Nymwill render possible. If the internet is the collective mind of humanity, then, as the song goes—free your mind and the rest will follow.

> *“Our masters have not heard the people’s voice for generations and it is much, much louder than they care to remember.”*
>
> -V FOR VENDETTA, ALAN MOORE

NYM

Web
Nymtech.net

Email
info@nymtech.net

Twitter
@nymproject

Github
@nymtech