Press Kit

13.03.2025

Table of contents

Media Resources

Nym Visual Assets
Download Logos, Headshots, Screenshots

What is Nym?

Company overview

About Nym

Nym thinks that all of humanity should be able to access the internet privately and without interference. Unfortunately, in the age of data surveillance, artificial intelligence (AI), and global censorship, being private online is increasingly impossible. So Nym has created privacy-preserving software and a surveillance-resistant, decentralized network for people and developers across the world.

Nym's journey begins with innovations like NymVPN, the first Virtual Private Network (VPN) that protects users from advanced government and corporate surveillance, including AI-driven metadata tracking. The center of NymVPN is its Noise Generating Mixnet (NGM) to combat AI-surveillance.

Nym was founded in Switzerland by some of Europe's leading online privacy researchers, engineers, and activists, including Harry Halpin (MIT), Ania Piotrowska (University College London), Claudia Diaz (KU Leuven), and Alexis Roussel. Security and privacy advocate, Chelsea Manning, also works with Nym as a security consultant.

About NymVPN

NymVPN was designed to offer people genuine anonymity where all other privacy solutions come up short. It uses a first of its kind decentralized **Noise Generating Mixnet** architecture to make online traffic and metadata as untraceable as possible. After more than 40 years of research on and attempts to create mixnets, Nym's NGM is the first general-purpose mixnet available to route all user data through a global network of mixnodes. In addition to protecting users from government and corporate surveillance (including AI-driven metadata tracking), NymVPN also helps to circumvent censorship, protect against cyberattacks, and anonymize and secure cryptocurrency transactions.

NymVPN

Using NymVPN

NymVPN offers two modes to fully protect people's online identity while providing flexibility relative to protection needs and upload-download speeds.

1. Best-in-class privacy is ensured in the **Anonymous Mode**, which provides anonymity for users via the NGM. What makes NymVPN unique is its ability to secure metadata (IP addresses, timestamps, traffic patterns, etc.), which is left exposed by all other VPN technologies.
2. The Fast Mode based on **AmneziaWG** is best for general internet browsing, streaming, and sharing. It offers comparable speeds and higher levels of security than most traditional VPNs by routing traffic through two independent servers. It also helps protect against censorship of VPN use via Deep Packet Inspection.

Zero-knowledge proofs unlink user payment information from usage of the app, so anyone — including Nym Technologies and the payment processor — can't connect payments to what people do online.

NymVPN features & benefits

Noise to protect metadata and traffic patterns

The Noise Generating Mixnet shields both IP addresses and traffic patterns by adding "noise" to the network. Starting from multi-layer encryption of identically-sized data packets, noise includes cover or "dummy" traffic to increase the anonymity of the whole network, data packet mixing of different users, and as a result timing obfuscation of when packets arrive and leave each server.

Zero-knowledge network

No single entity on the decentralized Nym network can access a user's entire traffic route, making people's identity **unlinkable to what they are doing online**. Nym never has any access to a user's traffic records, not even to a user's identity when using the network. And node operators sign no logs policies, but never have access to a user's content or full traffic route.

Anonymous access credentials

NymVPN employs zero-knowledge proofs (called "**zk-nyms**") to enable users to verify payment without revealing their identities in accessing and using the Nym network. This makes it impossible for Nym or node operators to connect payment information to the usage of NymVPN.

Censorship resistance

With a growing team of researchers on censorship resistance behind the technology, NymVPN allows users to select the locations where they enter and leave the network. NymVPN's Fast Mode is also based on the AmneziaWG protocol to help fight censorship and surveillance via DPI.

Token-incentivized network

Nym's network is run by independent people all over the world who share a mission: make the internet private by default. Contributors are rewarded for their work through a novel **tokenomics model** powered by the NYM token. While users can pay for NymVPN in any fiat currency, all payments will be automatically converted to NYM tokens to provide anonymous access credentials while using the app and support the NYM tokenomics ecosystem.

NymVPN pricing & payments

NymVPN is now available for all major operating systems. Android and iOS apps are available via Google Play and the Apple App Store. MacOS, Linux, and Windows desktop versions are available for download on Nym's website. U.S. pricing starts as low as $5.49 a month with a 2-year subscription.

Subscriptions to NymVPN can be made easily in debit & credit cards (via Stripe) or in NYM tokens. The ability to pay in other crypto currencies like BTC and with privacy coins like Monero & Z-cash will be possible soon.

The Nym network

The Nym network is a global, decentralized community of people operating independent servers with Nym software. These “nodes” are run by privacy-enthusiasts around the world contributing to the Nym mission of bringing real online privacy to everyone.

Nym network operators (whether functioning as gateways or mixnodes) are incentivized through a NYM tokenomics program to provide quality service in handling user data through the Nym NGM. The more people who pay to use the Nym network, the more Nym operators are rewarded, and the more private and efficient the whole network becomes.

Nym funding and investors

Nym has raised $52 million and is backed by prominent investors including a16z, Binance, Polychain Capital, Eden Block, and the European Commission.

Leadership & spokespeople

Harry Halpin, PhD – CEO & co-founder

Alexis Roussel – Chief Operating Officer (COO) & co-founder

Claudia Diaz, PhD – Chief Scientist & co-founder

Ania M. Piotrowska, PhD – Head of Research & co-founder

 Jaya Klara Brekke, PhD – Chief Strategy Officer (CSO)

 Mark Sinclair, PhD – Chief Technology Officer (CTO)

 Marc Debizet – Head of Product

 Robinson Jardin – Head of Marketing

 Chelsea Manning – Security Consultant

Nym resources

- Nym.com
- Nym Blog
- Nym YouTube
- What is NymVPN?
- Nym is more than a VPN
- Nym's zero-knowledge network: No logging promises needed
- NYM token flow
- What is the Anonymous Mode in NymVPN?
- What is a mixnet?
- AmneziaWireGuard
- WireGuard VPN encryption
- Trust Center

NymVPN Specifications

Last updated 12 March 2025

Supported platforms

Android macOS Linux iOS Windows

Minimum system requirements

Android

Android 7 (Nougat) and later; NymVPN is currently not supported in AndroidTV

iOS

iOS 16 and later

Linux

.deb package (Ubuntu v22.04 and later, other Debian-based distributions), AppImage (any Linux distribution supporting AppImage), AUR packages (Arch Linux and Arch-based distributions), Flatpak

macOS

macOS 13 (Ventura) and later

Windows

Windows 10, Windows 11

NymVPN modes

Fast Mode

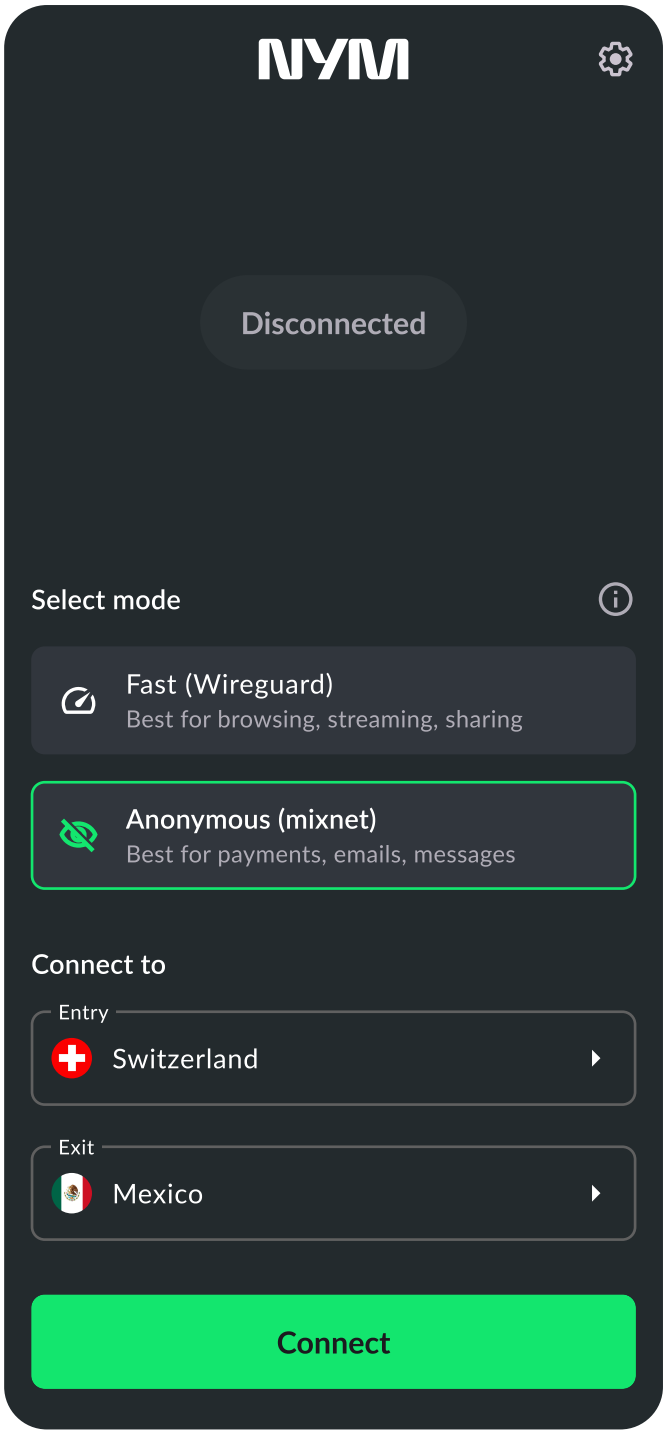
A 2-hop decentralized VPN in which user traffic is routed through an entry node and exit node respectively. The Fast Mode relies on the state-of-art AmneziaWG routing protocol.

Best use cases: Privacy for general browsing and streaming

Anonymous Mode

A novel 5-hop routing procedure through the Nym mixnet for highly private and anonymous online activity. With the mixnet, identically-sized and multi-layer encrypted data packets pass through an entry gateway to validate credentials, three subsequent mix nodes which further anonymize user traffic with noise, and an exit gateway that forwards encrypted data packets to their destination on the web. The mixnet also employs noise-generating network techniques (like cover traffic, data mixing, and timing delays) to combat network surveillance.

Best use cases: Private emailing, messaging, and crypto transactions



Opt for the fast decentralized VPN or prioritize higher privacy with the mixnet

Server types and specialties

All routing servers on the Nym network are operated by independent service providers who are incentivized to provide quality network services for NymVPN users. They are not employees or properties of Nym Technologies.

There are three types of network servers/functionalities:

Entry gateways

The entry point of the user with the Nym network

Mix nodes (only in the 5-hop mixnet mode *)

Three nodes which mix, delay, and anonymize user traffic in the Anonymous Mode

Exit gateways

The last step in the journey which forwards user data packets to their destination on the web

** Mixnodes are exclusively used in the mixnet for the Anonymous Mode, not the NymVPN Fast Mode. However, a node operator can choose whether they are functioning as an entry/exit gateway (for higher rewards) or as a mix node.*

Current number of locations and nodes (March 2025)

Locations covered

As of February 2025, about 63 locations are covered by entry/exit gateways. Mix nodes are located in over 80+ locations worldwide for maximum speed and resilience.

Total servers/nodes

125 gateways and 555+ mixnodes

Nodes per location:

Varies, with specific examples including:

USA: 75+

Germany: 70+

Others

Detailed server counts per locations are available, with servers strategically placed to ensure high speed and reliability:
https://harbourmaster.nymtech.net/

Security protocols

The NymVPN Fast Mode and Anonymous Mode use different security and encryption protocols.

Fast Mode

The Fast Mode uses the AmneziaWG protocol, a fork of WireGuard.

While WireGuard and AmneziaWG are not designed specifically for decentralized networks, they have been further adapted on NymVPN:

- 2-hop setup by default, with a “tunnel in a tunnel” encryption for added privacy
- Decentralized PKI (Public Key Infrastructure) relying on Nym’s infrastructure

Default WireGuard cryptographic primitives:

- **ChaCha20** for symmetric encryption, authenticated with Poly1305
- **Curve25519** for ECDH
- **BLAKE2s** for hashing and keyed hashing
- **SipHash24** for hashtable keys
- **HKDF** for key derivation

Anonymous Mode

The Anonymous Mode routes traffic through the **Sphinx** encrypted routing protocol, which is designed to handle mixnet traffic with multi-layered encryption. This protocol requires 5 distinct encryption layers for the 5 network hops traffic makes through the mixnet (i.e., onion encryption), with each server only able to decrypt the outermost layer of encryption destined for it.

Sphinx cryptography

- **AES128** for secure communication between clients and entry nodes, as well as for encryption of the Sphinx header
- **BLAKE3** for key derivation in Sphinx packet format
- **Lioness** for encryption of Sphinx payload

Noise Generating Mixnet protections

Nym's signature privacy-ensuring technology is the Nym NGM which involves adding network noise to combat surveillance and metadata tracking.

- **Uniform data packets:** User traffic is prepared into identically sized and uniform data packets (of 2KBs) to make traffic analysis based on differing packet sizes extremely difficult.
- **Cover traffic:** The NymVPN client introduces "empty" or "dummy" data packets into the network to increase the anonymity set for all users (i.e., the traffic volume of the mixnet).
- **Data mixing:** As user data packets arrive on a mix ode, the mixnode shuffles together the packets of different users before rerouting, confusing correlations between inputs and outputs.
- **Timing obfuscations:** When the data packets handled by a mixnode are mixed together, delays are introduced to obscure when packets leave the server.

Key privacy benefits of NymVPN

Unlinkable online activity

Prevents the correlation of your IPs with network requests, ensuring a robust safeguard against unauthorized access to your traffic and private data

- **Unlinkable payment system:** Conceals your identity when buying the subscription thanks to zero-knowledge access credentials (zk-nyms)
- **Zero-knowledge proof access:** Enables unlinkable activity by access to the network without revealing sensitive information.

Traffic analysis resistance

Prevents metadata surveillance of the users through the network based on sophisticated and AI-powered data tracking.

Zero-knowledge network design

Is decentralized with no centralized point in the entire network where full logs of user traffic can be kept to link a user with their destination.

Kill switch

Cuts your internet connection if the encrypted tunnel with the VPN gateway is interrupted even temporarily to prevent unnoticed data leaks.

Censorship resistance

Protects against censorship surveillance of VPN use by Deep Packet Inspection by default through AmneziaWG on the NymVPN Fast Mode.

Yearly network security audits

Open source code most recently performed by Cure53 in July 2024.

Gateway selection

Choose not only the location of entry and exit gateways, but the particular node based on its performance score and stake in the network.

Open source

Is fully transparent, open to public contributions and scrutiny.

World-class privacy and cryptography team

Benefits from the support of an elite team with PhDs, peer-reviewed work, and strong academic credentials (e.g., INRIA, KU Leuven, MIT, UCL).

Swiss headquartered

Benefits from Swiss jurisdiction and data regulations, for maximum protection.

Upcoming NymVPN features in 2025

Split tunneling

Customize which traffic uses NymVPN, what bypasses it, and which traffic and apps use each mode to balance anonymity protections with speed.

Post-quantum cryptography

Quantum-encrypt your data for long-term protection against the AI and super-computers of the future.

Ad blocker

Stop invasive ads and trackers from connecting with your device or software.

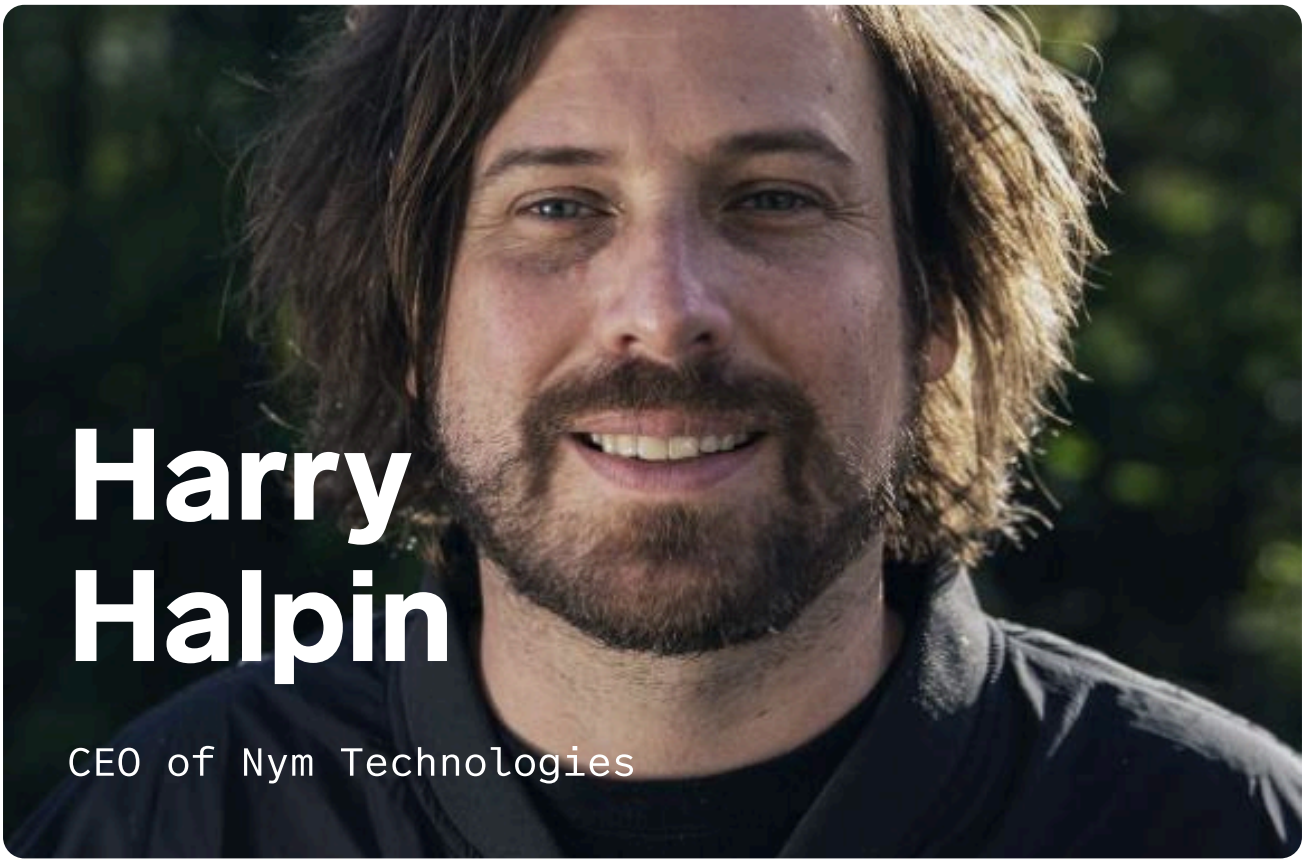
Improved censorship resistance

Tools that protect against VPN use being detected and blocked.

Nym policies

- **Legal disclaimers or terms of service**
- **Planned features and upcoming updates**
- **Data handling policies and practices**

Leadership & Spokespersons



Harry Halpin, PhD, co-founder and CEO of Nym, is a renowned technologist and privacy advocate. Harry leads Nym's development of cutting-edge, decentralized technology aimed at protecting digital privacy from mass surveillance and censorship. Nym's technology has gained significant traction among activists and political exiles in regions as diverse as Ukraine and Syria, offering a level of internet privacy unmatched by all conventional VPNs.

Harry’s journey

Harry's commitment to privacy-preserving technologies is deeply personal. His journey began after becoming a target of police surveillance in the UK, where undercover police officer Mark Kennedy infiltrated activist groups protesting government inaction on climate change with whom Harry was participating. Kennedy placed Harry on a blacklist, trying to prevent him from being hired at MIT by Tim Berners-Lee, the inventor of the Web. Following the UN climate summit in Copenhagen in 2009, Harry was assaulted by Danish police and arrested, although charges were dropped in court. These experiences inspired Harry to switch his career from research in AI to developing tools that empower individuals to reclaim their digital privacy.

Prior to founding Nym, Harry worked extensively in academia and left a tenure-track professorship offer to found Nym. Harry holds a Ph.D. in Informatics from the University of Edinburgh under Andy Clark, a well-known philosopher of AI. Harry completed his post-doctoral studies under Bernard Stiegler, France's leading philosopher of technology.

Privacy activism

As a researcher at MIT, Harry led the standardization of the Web Cryptography API, implemented across all major browsers and decentralized social media at the World Wide Web Consortium. At Inria de Paris (France's national research center for computer science), he led the European Commission's NEXTLEAP project on the socio-technical aspects of privacy and surveillance. More recently, he taught cryptocurrency at the American University of Beirut as hyperinflation engulfed Lebanon. He has published over 100 peer-reviewed publications across philosophy, AI, social media, and cryptography.

Beyond his technical expertise, Harry is a vocal critic of mass surveillance and AI. He was one of the founding advisory council members of the Progressive International and regularly works in-person with journalists and high-risk activists in the Middle East, Asia, and Africa. His work and advocacy have helped many to stand up for their digital freedoms, establishing him as a leading figure in the global privacy movement.

Alexis Roussel is the chief operating officer (COO) of Nym where he spearheads efforts to protect digital privacy via decentralized technologies. His work is firmly rooted in the intersection of technology and governance. Under his leadership, Nym has pioneered innovative solutions like the Nym mixnet which offers robust defenses against digital surveillance by obscuring communication patterns.

Alexis' journey

Alexis co-founded Bity.com, one of Switzerland's first crypto-finance service providers. He also served as an e-Governance Specialist for the United Nations where he integrated technology into governance systems to enhance transparency and citizen participation.

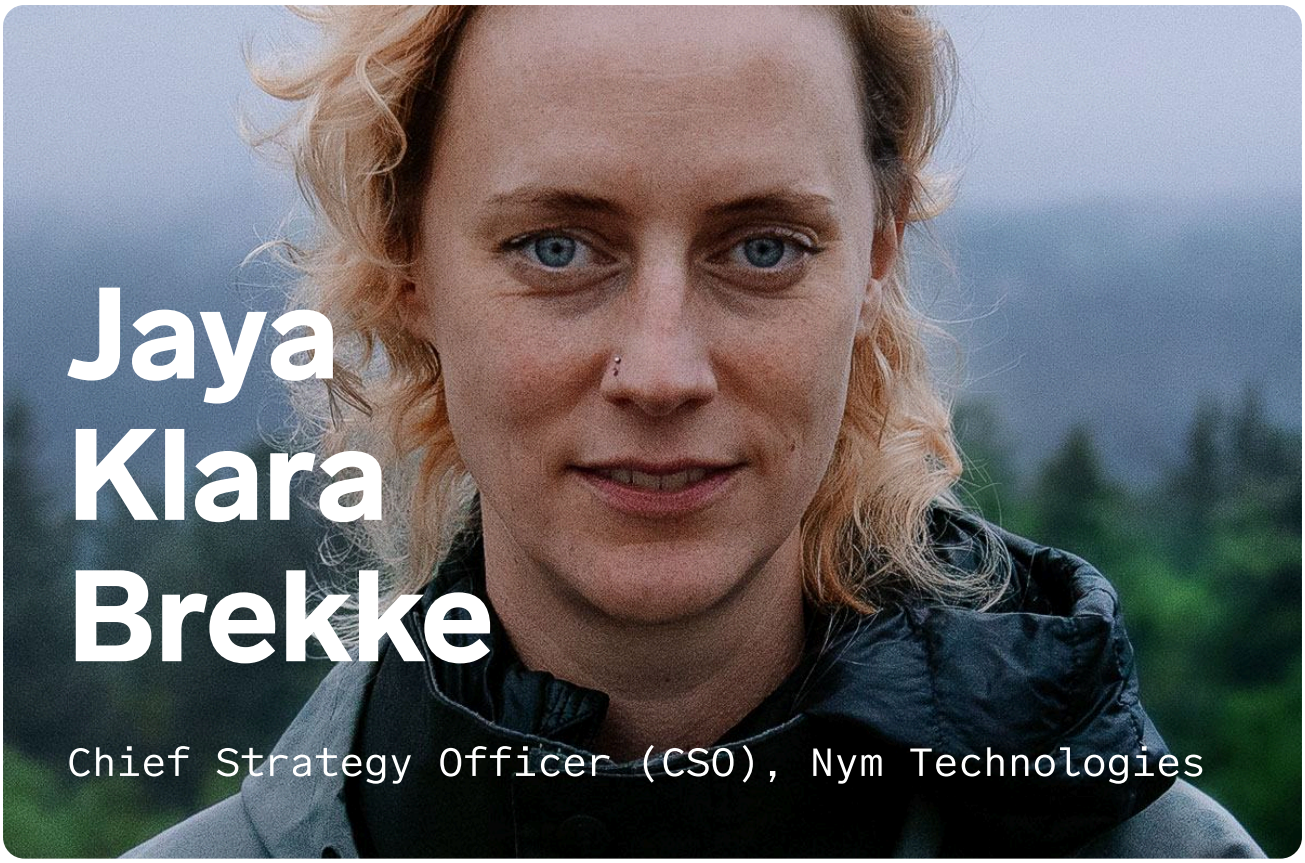
As former president of the Pirate Party of Switzerland, Alexis has been a vocal advocate for digital rights and a human-centric approach to technology.

His leadership in the party is a testament to his dedication to promoting decentralization and empowering individuals in the digital era. Alexis has also co-champions recognizing digital integrity as a fundamental human right. This concept was successfully integrated into law in Geneva.

Alexis is dedicated to advancing privacy-enhancing technologies at Nym, particularly in cryptocurrency transactions. He firmly believes in the necessity of anonymity and the right to avoid surveillance, arguing that these are essential for preserving democracy and individual freedom in the increasingly digital world.

Privacy and democracy

Alexis' work is propelled by a profound belief that privacy is not just a personal preference but a cornerstone of democratic society. His unwavering commitment to developing technologies that enable individuals to maintain sovereignty over their personal data and digital identities is evident in his endeavors at Nym and beyond. Alexis emerged as a leading figure in the global movement to protect digital privacy and integrity, advocating for a future where individuals can engage online without the fear of surveillance or data exploitation.



Jaya Klara Brekke, PhD, is the Chief Strategy Officer (CSO) at Nym where she plays a pivotal role in developing advanced privacy-enhancing technologies. With a PhD from Durham University, her research delves deeply into the political economy and the governance of decentralized technologies, particularly blockchain. Jaya's work is characterized by a commitment to exploring the ethical dimensions of technology, focusing on how power and control manifest within digital infrastructures.

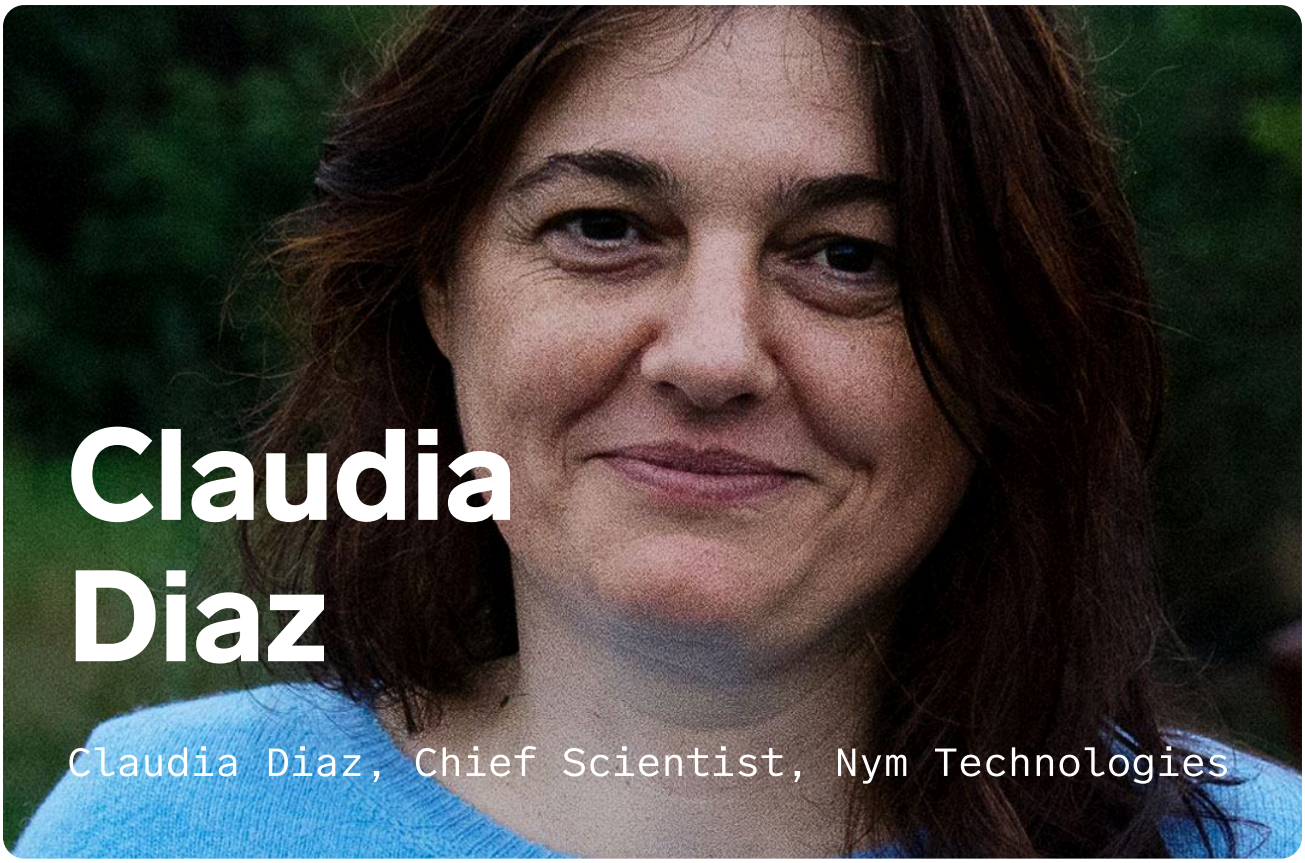
Jaya's journey

Before joining Nym, Jaya was actively involved in several high-profile projects, such as DECODE and D-CENT, which focused on democratic control over digital data. Her interdisciplinary expertise spans research, design, and policy, making her a sought after advisor on digital strategy and governance. She has also contributed to various academic and cultural initiatives, further solidifying her reputation as a thought leader. Jaya's work has earned her recognition and fellowships, including a prestigious position at the Weizenbaum Institute in Berlin.

In addition to her professional achievements, Jaya has served as an advisor to the European Commission on matters related to digital policy, emphasizing the importance of individual privacy and data sovereignty. Her insights into the complex interplay between technology, politics, and society have been published in numerous journals and platforms where she discusses the implications of emerging technologies on privacy and democratic governance.

Privacy advocacy

Jaya's commitment to ethical technology design is not just theoretical, but deeply practical. She aims to empower individuals and communities to reclaim control over their data in an increasingly surveilled world. Through her work at Nym and beyond, Jaya's actions and initiatives inspire others to advocate for technologies that prioritize privacy and human rights. Her influence extends beyond her immediate work, establishing her as a pivotal figure in the global discourse on digital sovereignty and privacy, shaping the future of technology and its impact on society.



Claudia Diaz, PhD, is the Chief Scientist at Nym where she leads the development of cutting-edge privacy-enhancing technologies to secure online communications. She also works part-time as Associate Professor at the COSIC research group at KU Leuven where she spearheads research in privacy technologies.

Claudia's journey

Claudia earned her PhD in engineering from KU Leuven, with a dissertation focused on the anonymity and privacy of online communications. Her research interests include anonymous communication systems, traffic analysis techniques, and secure decentralized systems.

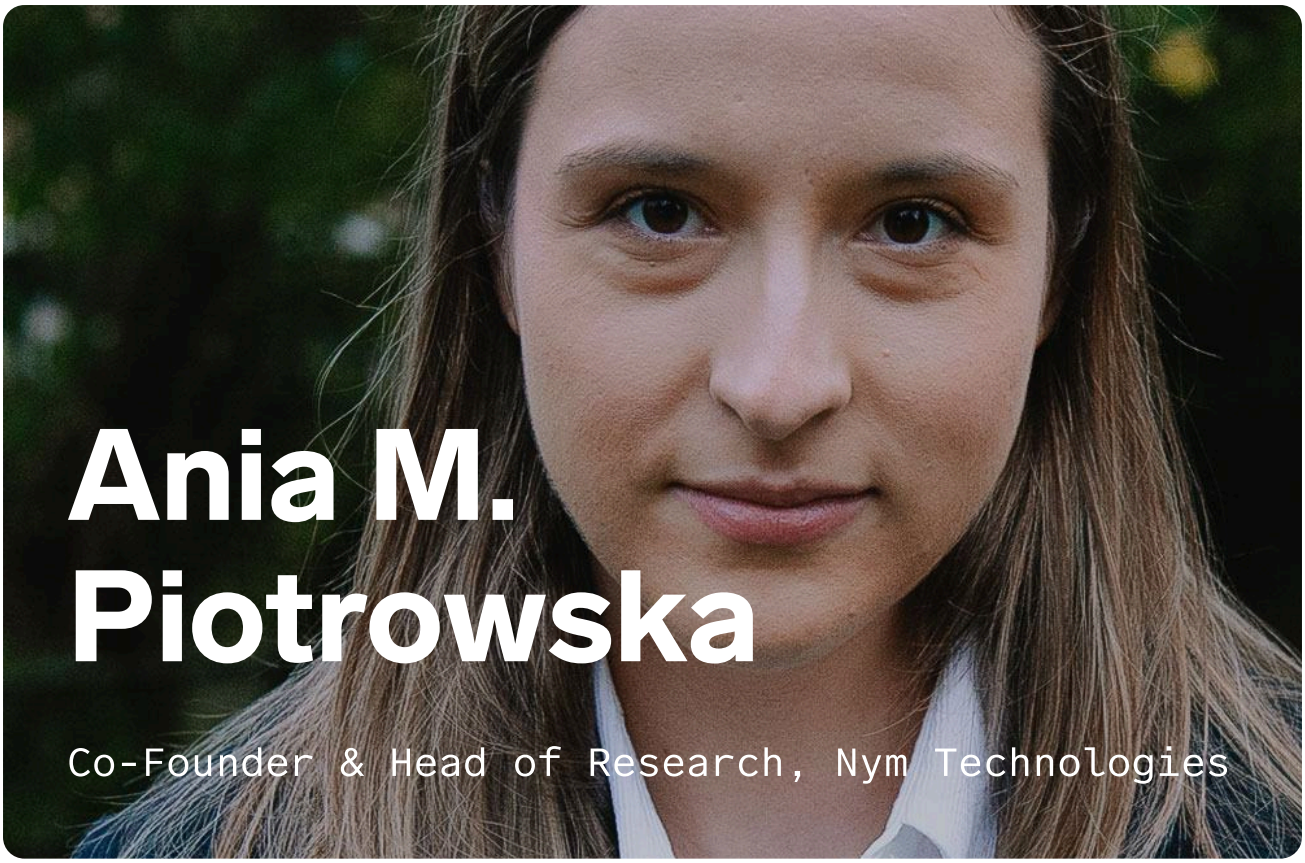
Before joining Nym, Claudia played a key role in various high-profile research initiatives, including EU-funded projects focused on privacy, security, and decentralized technologies. At Nym, she has been instrumental in advancing the development of incentivized mixnets — anonymity networks that obscure metadata and protect users from traffic analysis and surveillance, showcasing her practical contributions to the field.

At Nym, she has been instrumental in advancing the development of incentivized mixnets — anonymity networks that obscure metadata and protect users from traffic analysis and surveillance, showcasing her practical contributions to the field.

Privacy research and advocacy

Claudia is widely recognized for her academic work in privacy technologies, having published dozens of peer-reviewed papers and been a prominent voice in forums on privacy rights and security measures. Her insights into metadata protection and decentralized privacy solutions have established her as a thought leader in the privacy tech space, making her a sought-after expert for consultations on privacy infrastructure and digital rights.

In addition to her academic and professional roles, Claudia actively participates in advisory boards and steering committees related to privacy-enhancing technologies. Her commitment to advancing the field is further evident in her work at Nym where she focuses on both theoretical research and the development of practical tools to empower individuals and protect digital privacy in an increasingly surveilled world. Through her contributions to Nym and her ongoing academic efforts, Claudia plays a pivotal role in the global conversation around privacy, metadata protection, and secure communication infrastructures.



Ania M. Piotrowska, PhD, is the co-founder and Head of Research at Nym where she plays a pivotal role in developing privacy-enhancing technologies to secure online communications. Her work focuses on building systems that protect user anonymity and mitigate surveillance, particularly through mix networks and other cryptographic tools. Under Ania's leadership, Nym is reshaping how privacy is perceived and implemented in decentralized technologies.

Ania's journey

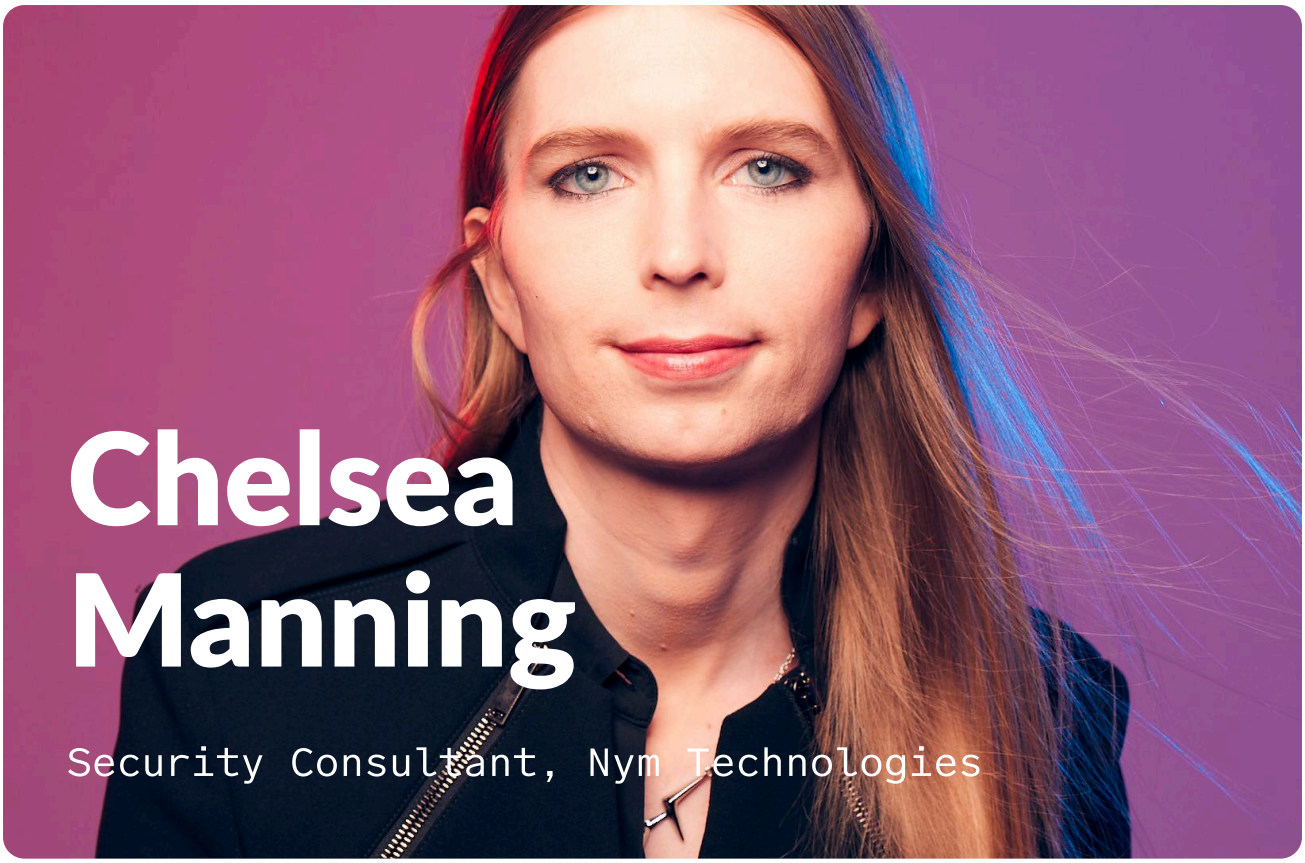
Ania earned her Ph.D. in computer science from University College London (UCL) where she was mentored by Professors George Danezis and Sarah Meiklejohn. Her doctoral research, titled "Low-latency Mix Networks for Anonymous Communication," has made significant contributions to the field of information security. Ania is a recognized authority in her domain, with a track record of publications in top security venues and professional experience gained through internships at leading organizations such as DeepMind and Chainalysis.

Before her work at Nym, Ania completed her MSc and BSc in computer science at Wrodaw University of Science and Technology, specializing in algorithm analysis. Her career is defined by a deep passion for strengthening user privacy in both theoretical and practical contexts, with a particular focus on the potential of blockchain technology to enhance privacy in cryptocurrencies. At Nym, Ania remains dedicated to advancing anonymous communication technologies and contributing to the development of privacy-preserving infrastructures.

Privacy research

Ania's contributions have solidified her reputation as a leading researcher and advocate in the privacy space. Through her work at Nym, she continues to shape the future of secure digital infrastructures, empowering individuals and organizations to protect their privacy in an increasingly interconnected world.

She is currently leading technical research projects to improve the Nym mixnet, as well as censorship resistance technologies to address the growing problem of VPN censorship practices around the world.



Chelsea Manning is the security consultant at Nym where she leverages her extensive background in network security and cryptography to advance the company's mission of enhancing online privacy. Known for her pivotal role in the 2010 Wikileaks revelations, Chelsea has since transitioned her focus to developing and securing privacy-enhancing technologies.

Work at Nym

At Nym, Chelsea is critical in conducting thorough security audits and identifying potential vulnerabilities in the company's network. Her work involves refining Nym's privacy infrastructure, ensuring it can withstand sophisticated attacks from state-level adversaries. Chelsea's expertise in network traffic analysis and blockchain technology is central to Nym's goal of creating a robust, decentralized privacy solution that goes beyond the limitations of existing tools like Tor.

Chelsea's contributions extend to developing innovative techniques to obscure and protect data traffic, incorporating blockchain-based methods to enhance the security and anonymity of users. Her work at Nym continues her commitment to defending privacy in the digital age, applying her insights to build more resilient and secure online environments.

Privacy advocacy

In addition to her technical work, Chelsea is a key advocate for privacy rights, bringing a critical perspective to Nym's development strategies and helping to navigate the complex challenges of building privacy tools in a world increasingly dominated by surveillance. Her ongoing work at Nym is instrumental in positioning the company at the forefront of the global movement for online privacy and data security.

Thank you

Contact

contact@nym.com

Media Inquiries

darija@nymtech.net

Social media

X

Youtube

Community channels

Matrix

Telegram

Discord