NYMVPN

Press Kit

Table of contents

What is Nym?

Company Overview

● Nym Technologies

Nym Technologies is a Swiss-based company pioneering the next generation of online privacy tools. Their flagship product, NymVPN, is an open-source application designed to provide users with the most advanced anonymity currently available. Through decentralization, a token-incentivized network, and mixnet technologies, Nym offers a novel solution to the problem of online privacy in the age of AI-powered surveillance.

● Mission Statement

To enable digital privacy for all humanity.

● Vision Statement

Nym aims to make privacy online a reality in the age of data surveillance, Artificial Intelligence (AI), and global censorship by delivering privacy-preserving software and a decentralized network to users and developers across the world.

● Investors

Nym Technologies is backed by prominent investors including a16z, Binance, Polychain Capital, Eden Block, and the European Commission.

NymVPN

● Overview

NymVPN is the first VPN in the world to offer true online privacy. It uses a unique Noise-Generating Mixnet (NGM) architecture to ensure that users remain unlinkable to what they do online. With its flagship Anonymous Mode, the network multi-layer encrypts user traffic into indistinguishable packets and routes them through five layers of the Nym mixnet. In the mixnet, different users' data packets are mixed together along the way to make them untraceable. It also adds "noise" to the network to obscure patterns of communication against AI surveillance.

● Key Benefits of NymVPN

Unlinkable traffic

Thanks to a decentralized network, users are unlinkable to their traffic online so they can go about their online business privately without worrying about metadata surveillance and exploitation.

Zero-knowledge network design

Nym Technologies never has access to data about what users do online, and network operators never have access to full logs that could link a user's identity to their destination on the web.

Unlinkable payments

Utilizes novel zk-nyms anonymous credentials which delinks a user's payment for NymVPN from their access to and use of the network.

Customizable privacy

User-friendly interface allowing customization of privacy preferences, including whether to use the advanced Anonymous Mode or the faster and still decentralized Fast Mode.

● Unique Value Proposition

No other VPN on the market can protect against AI-powered surveillance of a network which can reveal our patterns of communication. NymVPN can safeguard everyone's personal information, metadata records, and digital autonomy through decentralized, mixnet, and noise-generating network technologies.

● Key Commitments

- Nym Technologies never has access to user traffic records

- Users will always remain unlinkable to their activities on the web

- Users cannot be linked to their usage of the app from their payment records

● User Experience

- Decentralized, multi-hop routing by default

- Choice of level of anonymity protections to optimize speeds when needed

- State-of-the-art encryption to prevent spying and hacking.

● Key Use Cases

General users: Protect metadata records

Metadata records are globally harvested for commercial and surveillance purposes.

Access foreign content

Choose your entry and exit locations to access contents not available in your country.

Bypass censorship restrictions

Acting as a shield to bypass restrictions and access blocked content freely.

Positioning

- ## What Nym Does

NymVPN is the first VPN in the world to offer true privacy against the most advanced surveillance techniques.

- ## Who Nym Does It For

NymVPN and the Nym network is designed for everyone: tech enthusiasts, privacy advocates, journalists, activists, developers, and individuals seeking enhanced online privacy and security.

- ## Why Nym is Different

The large majority of VPNs do not actually protect people's privacy and metadata, especially given new AI capacities. Nym is the first VPN to run a mixnet to offer users an unparalleled level of security and anonymity on the internet that even AI can't penetrate.

Leadership & Spokesperson Bios

 Harry Halpin - CEO & Co-Founder

 Alexis Roussel - Chief Operating Officer (COO)

 Claudia Diaz - Chief Scientist & Co-Founder

Jaya Klara Brekke - Chief Strategy Officer

Anna M. Piotrkowska - Co-Founder & Head of Research

Mark Sinclair - Chief Technology Officer

Marc Debizet - Head of Product

Chelsea Manning, Security Consultant

Key Messages

More than a VPN:

NymVPN is a decentralized network, a community-powered project, a technological solution to AI surveillance, a token-incentivized infrastracture, and an activist initiative to make the internet private by default.

Private together:

Nym is a community of developers, privacy enthusiasts and researchers, independent operators, token holders, activists, and people dedicated. Moreover, every user of the Nym network increases the overall anonymity of others. Online privacy is achieved together and not alone.

Expert Backing:

Nym is backed and built by key researchers, scientists, figureheads, developers, and authorities in the digital privacy and security space.

Public Relations FAQ

Nym Technologies

What is Nym Technologies?

Nym Technologies is a pioneering company focused on creating privacy-centric internet tools. Their flagship product, NymVPN, is a free and open-source application designed to provide users with complete anonymity as they navigate the internet.

What unique value does Nym Technologies offer?

Nym Technologies addresses the critical need for safeguarding personal information and digital

What is Nym's mission?

Nym Technologies aims to ensure privacy in the age of datafication and AI by making advanced privacy-preserving software available to developers and end users.

Who are the investors behind Nym Technologies?

Nym Technologies is backed by prominent investors including a16z, Binance, Polychain Capital, Eden Block, and the European Commission.

Who founded Nym Technologies? Who owns the company?

Nym was co-founded by Harry Halpin, Claudia Diaz, Dave Hrycyszyn, Alexis Roussel, Ania Piotrowska, Jedrzej Stuczynski, and Narges Dadkhah

Who is Harry Halpin? Why did he start Nym Technologies?

Harry Halpin co-founded Nym Technologies and is Nym's CEO. He founded Nym to provide genuine online privacy for the whole world.

NymVPN

What is NymVPN?

NymVPN is the first Virtual Private Network (VPN) in the world to offer true privacy. It uses a unique mixed network architecture to provide complete anonymity online by routing user data packets through a global network of mix nodes.

How does NymVPN ensure user privacy?

NymVPN utilizes a multi-layered approach: a fully decentralized network, up to 5-hops worth of IP address obfuscation, state-of-the-art layered-encryption, added network noise including dummy traffic and timing delays. Together these techniques make message content and metadata virtually untraceable. It also employs a strict no-log policy and never sells user data or IP addresses because, by network design, there is no central place where user metadata can be logged.

What are the key benefits of using NymVPN?

NymVPN offers completely untraceable digital presence, a user choice over their level of privacy, financial anonymity through zk-nyms, and solid token utility with the NYM token.

Who can benefit from NymVPN?

NymVPN is designed for tech enthusiasts, privacy advocates, developers, and anyone seeking enhanced online privacy and security. It also serves enterprises looking to integrate robust privacy tools into their security infrastructure.

What makes NymVPN different from other VPNs?

Unlike other VPNs, NymVPN uses a combination of decentralized technology and a mixed network to provide unparalleled security and anonymity. It ensures complete privacy by protecting traffic and metadata from surveillance and unauthorized data collection.

What are zk-nyms and how do they enhance privacy?

zk-nyms are anonymous credentials that enable secure and anonymous transactions. They allow users to make private payments using fiat or crypto without revealing their identities, ensuring financial anonymity.

When will NymVPN be available to the public?

NymVPN Beta is currently free and available to test for everyone. To be part of the Beta testing phase, simply sign up at **nymvpn.com/en.** The commercial app will be available for purchase in November 2024, with advanced features like WireGuard for the Fast Mode and anonymous payment methods.

How do I access NymVPN?

Signup for access to NymVPN Beta at **nymvpn.com/en**, download the app for your device, and get an instant credential to activate your access on your app.

How can journalists and members of the media trial NymVPN?

Any journalist or media person can signup for free access to NymVPN Beta at **nymvpn.com/en.** However, we highly encourage you to reach out to us at **contact@nymtech.net** for more information on the product, a tutorial on the app, and to hear about its current and coming privacy features.

Who runs the servers of the Nym network?

The Nym network of servers (whether 2-hops through the Fast Mode or 5-hops through mixnet Anonymous Mode) are independently owned and operated. They are not the employees of Nym, but privacy-enthusiasts around the world contributing to the Nym mission of bringing real online privacy to everyone.

What is the relationship between NymVPN and the NYM token?

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

NymVPN Specifications

Last updated November 7, 2024

● Supported platforms

Android: macOS: Linux: iOS: Windows:

● Minimum system requirements

Android:

Android v7 and later. NymVPN is currently not supported in AndroidTV

macOS:

macOS v13 (Ventura) and later

Linux:

AppImage (any Linux distributions supporting AppImage), Debian/Ubuntu v22.04 and later, .deb package (Debian/Ubuntu v22.04 and later), Arch Linu

iOS:

iOS v16 and later

Windows:

Windows 10, Windows 11
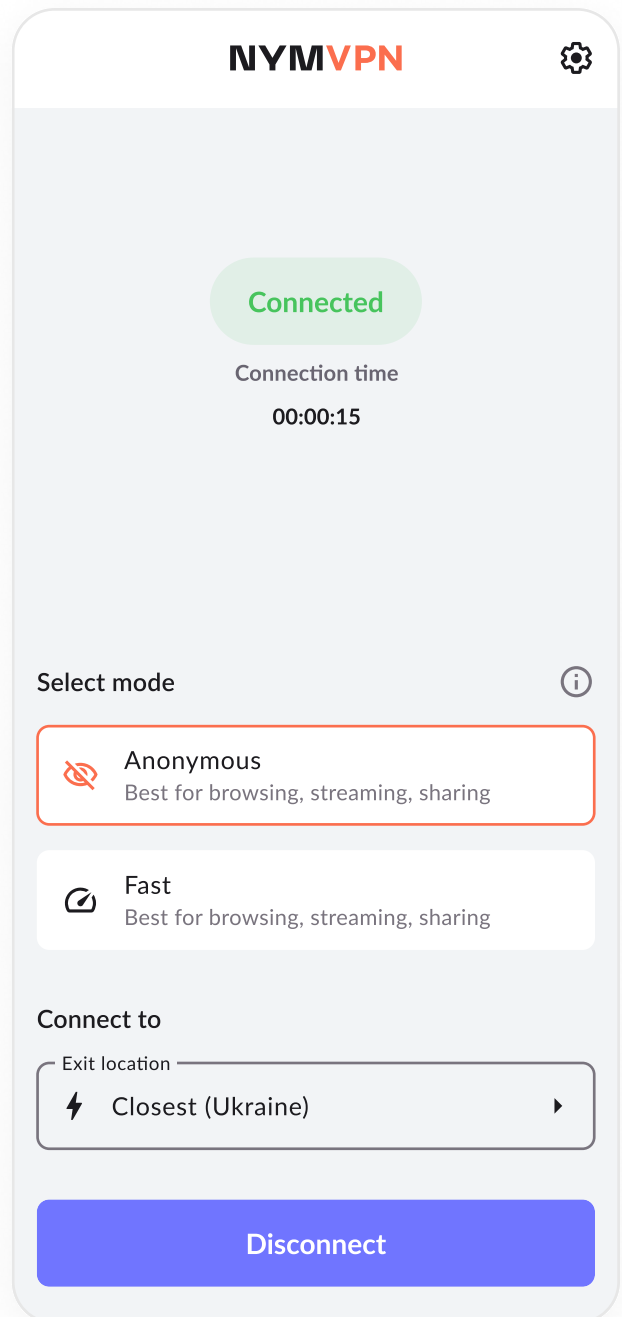
● NymVPN modes

◔ Fast Mode

A 2-hop decentralized VPN in which user traffic is routed through an entry node and exit node respectively. The Fast Mode is relying on the state-of-art WireGuard 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 mixnodes which further anonymize user traffic, 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 and timing delays) to combat against network surveillance.

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

NYMVPN   ⚙

Connected

Connection time
00:00:15

Select mode   ⓘ

◌ **Anonymous**
   Best for browsing, streaming, sharing

◔ **Fast**
   Best for browsing, streaming, sharing

Connect to

Exit location
⚡ Closest (Ukraine)   ▸

Disconnect

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

Mixnodes:

Three nodes which mix 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 mixnode.

Number of countries and nodes

Countries covered:

As of September 2024, about 30–35 locations are covered by entry/exit gateways. Mixnodes are located in over 80+ countries worldwide for maximum speed and resilience.

Total servers/nodes:

125 gateways and 750+ mixnodes

Nodes per country:

Varies, with specific examples including:

🇺🇸 **USA: 42+**

🇩🇪 **Germany: 17+**

🇯🇵 **Japan: 6+**

📍 **Others**

Detailed server counts per country 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 **WireGuard protocol.***

* WireGuard is currently being implemented and internally tested and will launch soon.

The WireGuard protocol is not designed specifically for decentralized networks, so there are particular modifications of the protocol 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, 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 network techniques

Nym's signature privacy-ensuring technology is the Nym mixnet 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 impossible.
- **Cover traffic.** The NymVPN client introduces "empty" or "dummy" data packets into the mixnet 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 node, the mix node mixes the packets of different users before rerouting, confusing correlations between inputs and outputs
- Timing obfuscations. Data packets handled by a mix node are mixed together, resulting in delays on when packets leave the server.

Key privacy benefits of NymVPN

Unlinkable online activity:

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

- **Privacy-preserving payments:** Conceal your identity when buying the subscription thanks to zero-knowledge credentials.
- **Network security audits:** Performed recently by Cure53 in July 2024
- **Zero-knowledge proof access:** What enables unlinkable activity is access to the network without revealing sensitive information, enhancing your privacy and security.

Traffic analysis resistance:

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

Zero-knowledge network design

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

Open source:

The NymVPN and mixnet codes are fully transparent, open to public contributions and scrutiny

World-class privacy and cryptography expert team:

Benefit 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:

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

● Comming features

* Currently in research and development

⤳ **Split tunneling**

⏻ **Killswitch and auto-connect**

▣ **Post-quantum cryptography**

📢 **Censorship resistance**

● Additional resources

Learn about NymVPN

- NymVPN
- NymVPN Blog
- What is NymVPN?
- What is the Anonymous Mode in NymVPN?
- What is a mixnet?
- WireGuard VPN encryption
- Sphinx mixnet encryption
- Trust Center

Nym policies

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

Leadership
& Spokespersons

Harry Halpin

CEO of Nym Technologies

Harry Halpin, co-founder and CEO of Nym Technologies, 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 Iraq, offering a level of internet privacy unmatched by 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 lack of action on climate change that Harry was involved with. 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 postdoctoral studies under Bernard Stiegler, France's leading philosopher of technology.

Privacy activism

As a researcher at MIT, he 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

Chief Operating Officer (COO), Nym Technologies

Alexis Roussel is the Chief Operating Officer (COO) of Nym Technologies, 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 mixnets, which offer robust defenses against digital surveillance by obscuring communication patterns.

Alexis' Journey to Nym

He 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.

The 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. He has also co-authored the book Our Precious Digital Integrity with Grégoire Barbey, which 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 Technologies, 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 Roussel's 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. He has 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

Chief Strategy Officer (CSO), Nym Technologies

Jaya Klara Brekke is the Chief Strategy Officer (CSO) at Nym Technologies, 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 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 to Nym

Before joining Nym, Jaya was actively involved in several high-profile projects, such as DECODE and D-CENT, which centered 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. Her 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

Claudia Diaz, Chief Scientist, Nym Technologies

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

Journey to Nym

Diaz 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, Diaz 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.

Privacy research and advocacy

Diaz is widely recognized for her academic work in privacy technologies, having published dozens of peer-reviewed papers and being 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, Diaz 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 Diaz plays a pivotal role in the global conversation around privacy, metadata protection, and secure communication infrastructures.

Anna M. Piotrowska

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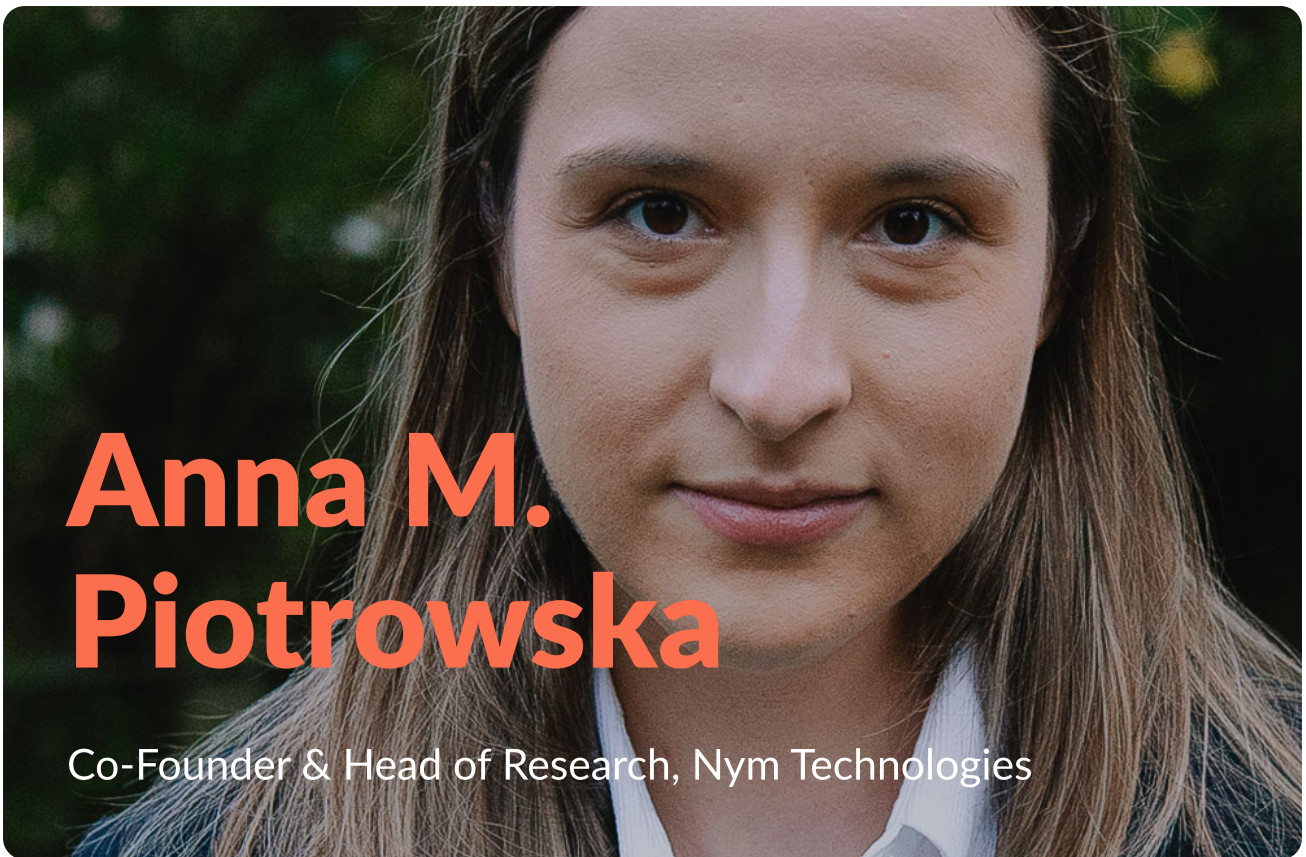
Ania M. Piotrowska is the Co-Founder and Head of Research at Nym Technologies, where she plays a pivotal role in developing privacy-enhancing technologies to secure online communications. Her work focuses on building systems that protect user anonymity and mitigate surveillance, particularly through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

Journey to Nym

Dr. Piotrowska 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. She 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 Wrocław 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, she remains dedicated to advancing anonymous communication technologies and contributing to the development of privacy-preserving infrastructures.

Research at Nym

Ania Piotrowska'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 compact the growing problem of VPN censorship practices around the world.

Chelsea Manning

Security Consultant, Nym Technologies

Chelsea Manning is the Security Consultant at Nym Technologies, 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. Her 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 Technologies is instrumental in positioning the company at the forefront of the global movement for online privacy and data security.

Thank you

Contact

✉ contact@nymtech.net

Media Inquiries

✉ nym@hokkupr.com

Social media

𝕏 X

▶ Youtube

Community channels

◎ Matrix

✈ Telegram

🎮 Discord