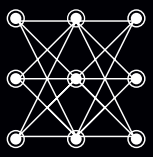
NYM

NymVPN Litepaper



Protecting patterns of communication for all internet traffic

Index

1

Introduction & Motivation

In an age where our lives are increasingly intertwined with the digital realm, safeguarding online privacy has become imperative.

The rapid increase in data breaches, cyberattacks, pervasive surveillance, and geo-blocking has highlighted the need for robust tools that empower individuals to reclaim their privacy, secure their digital footprint, and regain unrestricted access to the online world. For these reasons, now is the time to introduce the NymVPN app, a revolutionary platform that offers users access to a decentralised VPN and a decentralised mix network in a single application, providing the highest level of privacy and security for your online activities.

The Need for Online Privacy

The digital landscape is rife with threats, from cybercriminals seeking to exploit vulnerabilities to surveillance entities hoovering up personal data without consent. Moreover, governmental restrictions and online censorship in various regions not only stifle the free exchange of ideas but also hinder access to vital information. User privacy isn't merely a luxury, it's an essential shield against identity theft, intrusive tracking, and the erosion of our fundamental right to access information and express ourselves freely in the digital age.

Encryption or secure transmissions alone are not enough to safeguard online privacy. The protection of metadata – the data about your data – remains a formidable challenge. Metadata can reveal a great deal about your online behaviour, relationships, and even your state of mind, leaving you exposed to potential tracking and surveillance. Most existing technologies fall short of protecting metadata, leaving a critical gap in your privacy defences.

Centralisation: A Risk to Your Privacy

In the digital age, centralised solutions have become the norm. However, this comes at a cost in terms of your privacy and security. Traditional VPNs know your identity and your browsing history. Thus, entrusting your online privacy to a centralised entity exposes you to a single point of control, leaving your data exposed to potential breaches, harvesting and surveillance. Handing this trust to any one company creates a single point of failure and leaves your data vulnerable to breaches and surveillance. The need for a decentralised alternative becomes evident with the increasing frequency of data breaches and cyberattacks.

The Incentive Dilemma: Who Benefits?

In a world where data is power, incentivising individuals to actively participate in the protection of digital privacy becomes paramount. Traditional multi-hop networks often lack mechanisms for rewarding network participation, leaving node operators unmotivated. This void can create an environment where the quality and reliability of network nodes are inconsistent, and the interests of users may not be the primary concern. Free VPN services, in particular, often extract the cost of their "free" service from users' privacy and sell user activity to data brokers. Additionally, even in the case of Tor, which is a valuable tool for private communications, the quality of service varies because operators are not incentivised to provide consistent and reliable service – the network instead relies on goodwill.

Navigating a Sea of Privacy Solutions

In today's digital landscape, users face a perplexing conundrum when it comes to privacy. Various privacy tools offer different levels of protection, making them suitable for distinct use cases. For example, VPNs are often preferred for secure browsing, while onion routing and mixnets are lauded for their anonymity features. However, users are frequently tasked with juggling multiple applications, each tailored to a specific purpose. This complexity creates a fragmented approach to privacy and forces individuals to switch between applications, depending on their usage requirements. Adding to the complexity, users often lack a clear understanding of the specific privacy properties offered by different systems. The intricacies of encryption protocols, routing methods, and data-handling practices can be daunting, leaving many users uncertain about which tool to choose for their unique needs. As a result, making an informed choice about how to protect their digital lives becomes an uphill battle.

The Pitfalls of Traditional VPN Payment Systems

In the traditional landscape of VPN services, payment transactions are routinely interconnected with a user's online activities, leading to a trail of data that can be traced back to their digital footprint. This linkage poses a critical privacy risk, as it not only compromises the anonymity of users but also opens the door for third parties to potentially connect a user's identity with their specific browsing history and internet usage patterns. The implication of such visibility is far-reaching, often resulting in privacy infringement, unwarranted surveillance, and targeted profiling. The exposure of this sensitive information leaves users vulnerable to a range of security risks, including identity theft, data mining, and invasive advertising, fundamentally undermining online privacy and security. As a result, there is an urgent need for a more robust and privacy-preserving payment solution that ensures user identity is not connected to their online activities, preserving their digital autonomy.

2

Our Solution

In an era where the digital landscape is fraught with privacy concerns and data vulnerabilities, NymVPN emerges as a beacon of online privacy and security.

NymVPN is your trusted companion in the digital age, designed to address the pressing challenges faced by users seeking to safeguard their personal information, maintain their digital autonomy, and navigate the internet without compromise.

With the NymVPN app, we offer a robust solution that combines the power of a decentralised VPN and a decentralised mix network, ushering in a new era of online privacy protection. NymVPN ensures that your digital footprint remains secure and your online activities are truly private.

NymVPN: Your Gateway to Online Privacy

NymVPN offers unparalleled safety online. By combining encryption and metadata protections, NymVPN is the cornerstone of our commitment to ensuring digital privacy, security, integrity, and autonomy.

With NymVPN, you gain access to the Nym network—a revolutionary decentralised network of nodes managed by individuals, not central authorities. This network is the epitome of true decentralisation, where anyone can run a node, fostering a diverse ecosystem. This approach ensures that no single entity can compromise your privacy. The strength of the Nym network rests on its dedicated node operators, who are rewarded for their trustworthiness and reliable service. Powered by the NYM token, these incentives align the operators' interests with the community's security and privacy goals.

Our unique delegation mechanism gives NYM token holders the freedom to stake their tokens to node operators they trust. This democratic delegation process also serves as an impervious reputation system and a defence against Sybil attacks. Attempting to compromise the network's integrity through such tactics is arduous and futile, thanks to the transparent and democratic delegation system. For their participation and involvement in ensuring network integrity, delegators also receive a share of node rewards.

With over 600 nodes actively serving users in nearly 60 countries, the Nym network is a practical, global, and scalable decentralised system. Whether the user picks the dVPN or the mixnet mode, NymVPN ensures digital interactions are private and secure thanks to the powerful protection capabilities of the Nym network.

Streamlined Privacy in One Unified Solution

In today's digital world users are forced to pick from an array of fragmented solutions to achieve privacy. In contrast, NymVPN stands as a beacon of simplicity, bringing together a dVPN and a mixnet in one seamless application all powered by the same underlying network. The choice is up to the user: whether you need a multihop dVPN for everyday browsing or the full anonymity of a mixnet, NymVPN is a single integrated solution. No more switching between apps or navigating multiple networks – with NymVPN, privacy is a unified experience, simplifying access to a safer digital life

Total Control and Unmatched Privacy Across All Devices

NymVPN delivers uncompromising privacy across all your devices with its reliable full network protection service, safeguarding every online interaction. Setting NymVPN apart is its ability to automatically tailor privacy features to each unique use case, leveraging a unique combination of state-of-the-art mixnet and WireGuard VPN technologies. Unlike traditional VPNs, NymVPN doesn't limit protections to SOCKS5 – it covers your entire network connectivity, while a built-in kill switch provides additional safeguards should your connection drop. With split tunnelling, NymVPN allows users to choose whether app traffic is directed through the dVPN or the mixnet, while granular configurations mean greater user control over privacy preferences. All this power and convenience is integrated in one app, offering a holistic solution for all network connectivity needs. With NymVPN, your online privacy is not just a feature – it's a guarantee.

Cutting-edge and Secure Encryption at its Core

NymVPN protects your internet traffic from prying eyes with unbreakable encryption including AES-256, ChaChaPoly and Lioness. Whether you're sharing sensitive information, banking online, or simply browsing, your data is locked tightly out of reach from cybercriminals and online surveillance entities. This digital cloak safeguards your personal and sensitive information, shielding you from eavesdropping, data breaches, and identity theft.

Moreover, we are committed to the future of online security. While our encryption standards are already extremely strong, we aim to make them post-quantum secure, staying ahead of emerging threats and ensuring digital privacy even in the face of evolving technology.

Multi-hop Solution

BBeyond encryption, the NymVPN employs a multi-hop architecture that shields your digital identity from network tracking and enhances your security. Rather than routing traffic through a single proxy node like most VPNs, NymVPN takes the extra step of routing traffic via two independent proxy nodes in VPN mode, or five nodes in the mixnet mode – thwarting man-in-the-middle attacks and ensuring individual nodes on the path cannot link the user back to digital activities. This multi-hop approach adds an additional layer of privacy, making it significantly more challenging for websites, advertisers, and malicious actors to track your online behaviour. Your online identity remains safeguarded, ensuring that your digital privacy is fortified.

Access Without Boundaries

NymVPN is more than just a tool for online privacy; it's a commitment to a future where online freedom knows no boundaries. While our current iteration provides robust privacy solutions, we recognise that the fight for a truly open internet doesn't end here. We are dedicated to continuously improving and integrating novel and proven techniques that bolster NymVPN's resistance to censorship mechanisms.

Our goal is to empower individuals around the world, ensuring they have unfettered access to the information and resources they seek. As the digital landscape evolves, NymVPN will evolve with it, actively developing and implementing innovative methods to circumvent censorship and safeguard your online freedom.

Guarding Privacy with Untraceable Payments and Access

NymVPN addresses the critical challenges concerning payment privacy, ensuring users can access our services while safeguarding their digital identity. Our innovative zk-nyms technology offers an unparalleled zero-knowledge shield of transactions in any currency or cryptocurrency to pay for the service, preventing any correlation between user identity or payment information and the specific websites or services accessed within the Nym network. For example, payment in even Bitcoin could de-anonymize users via being linked to their NymVPN access, but zk-nyms convert any payment to NYM and provide an unlinkable "proof of payment" in zero-knowledge. With zk-nyms, paying for NymVPN services guarantees that neither node operators nor any external entities can link the user's identity with the websites or services they use.

3

Technical Overview

NymVPN empowers users by providing active access to the Nym network, a robust system designed to protect your online privacy.

The Nym Network Architecture

The Nym network is a decentralised ecosystem consisting of several key entities, each playing a vital role in ensuring the privacy and security of user activities.

Relay Nodes:
These nodes form the backbone of the Nym network. They are responsible for routing users' internet traffic through multi-hop paths, adding layers of privacy and security to online activities. Relay nodes are operated by independent individuals, each contributing to the network's powerful decentralisation.

Validators:
These validators play a pivotal role in maintaining the Nym blockchain, serving not only as a secure broadcast channel for distributing critical network-wide information but also as a decentralised public key infrastructure. Furthermore, the validators are responsible for distributing rewards to the node operators, ensuring the proper incentivisation of network participants

Nym-API Nodes:
Nym-API nodes have a distinct role within the network. They are responsible for issuing zk-nym credentials, a critical component of user access to the Nym network. These credentials serve as proof of payment for users' subscriptions and are essential for ensuring network participation.

Together, these entities form a decentralised, private environment where users can enjoy online activities without compromising their personal data or security.

Two Modes for Enhanced Privacy: dVPN and Mixnet

VPN Mode: The Power of Wireguard and Novel Onion Encryption
NymVPN offers you two distinct modes for safeguarding your online activities: the dVPN and the mixnet. In dVPN mode, your data traverses a secure 2-hop path, with each hop hosted by an independent operator. This setup combines the reliable Wireguard protocol, known for its high-performance encryption, with a novel layer-encryption scheme. Our choice of Wireguard ensures exceptional security and speed, making it an ideal choice for safeguarding your data while optimising for speed. The novel layer encryption scheme, which incorporates robust

cryptographic primitives, ensures data confidentiality and integrity and provides an additional layer of security, preventing the individual nodes routing the connection from correlating the user with their online activity. Additionally, it employs packet padding to ensure uniform packet sizes, adding an extra layer of security.

Therefore the dVPN mode provides a swift and high-speed online access solution, perfect for activities such as web browsing, gaming, and streaming. It excels at hiding your IP address from web servers and ensures there's no centralised point of control, thanks to its independent 2-hop structure.

While the dVPN mode offers strong privacy measures, it's important to note that it does not offer the same level of resistance against advanced traffic analysis attacks employed by sophisticated network adversaries.

Mixnet Mode: Advanced Privacy and Metadata Protection

For the use cases where users seek complete privacy protections, NymVPN's mixnet mode delivers robust security and takes users' privacy to the next level by offering traffic analysis resistance. In this mode, your data travels through a secure 5-hop path, with each hop introducing an extra layer of protection. To obfuscate your communication patterns, cover traffic is generated, injecting dummy packets indistinguishable from your normal traffic. What sets this mode apart is the advanced packet shuffling performed by the three inner nodes in the 5-hop path. This process ensures that packets cannot be correlated based on their timing, significantly enhancing privacy. As a result, the mixnet mode provides unparalleled security, even against sophisticated traffic analysis attacks. Even in the presence of global network observers or advanced machine learning attacks, this mode ensures your online activities remain confidential and shielded from prying eyes. Thus, it surpasses the privacy properties of traditional VPNs and Tor and is the fastest, most secure mixnet available today, keeping your online activities truly private.

Although the 5-hop path and additional security measures introduce longer communication latency compared to the dVPN mode, mixnet mode is an ideal choice for applications that prioritise privacy over low latency, such as sending cryptocurrency transactions, secure messaging, confidential emails or sharing of sensitive files.

Enhancing Privacy Through a Unified Network

By routing both dVPN and mixnet modes through the same underlying network, NymVPN offers an additional layer of privacy and security. This approach ensures that network observers are unable to differentiate between dVPN and mixnet traffic within the network, effectively obfuscating the flow of data. This integrated approach enhances user privacy by adding complexity for any entity attempting to monitor online activities.

Unlocking Privacy Across Diverse Digital Realms

NymVPN goes beyond securing web browsing by offering support for a diverse range of applications and services. Users can configure instant messaging (IM) and chat applications to connect to the Nym network via the NymVPN app, ensuring their private conversations are confidential. Similarly, email clients can be configured to route traffic through NymVPN, providing users with a secure and anonymous way to access and send emails. For cryptocurrency enthusiasts, NymVPN offers the option to connect cryptocurrency wallets, effectively preventing tracking of wallet addresses and transaction history. This expansive support ensures that users can enjoy the benefits of enhanced privacy across various online platforms and services.

In its current iteration, users can configure any applications, provided they support SOCKS5, to connect to the Nym network via the NymVPN app. Looking ahead, NymVPN is on the verge of an exciting development. In the near future, NymVPN will extend this capability to work with any IP traffic (ICMP, TCP, UDP) from any application.

Your Data, Your Rules: Mastering Privacy with Zero-Knowledge Credentials

NymVPN uses our cutting-edge zero-knowledge anonymous credentials called zk-nyms. This sophisticated cryptographic protocol combines the power of zero-knowledge technology with digital signatures to grant users access to the Nym network and its services without the need to unveil any sensitive information about their identity. When users opt for a subscription and make their payment in fiat, our system then transforms the payment into a buy order on the open market for NYM. Then our innovative payment system swiftly exchanges the NYM for zk-nyms credentials, which act as a kind of digital "proof of NYM payment" for secure and private transactions on the Nym network. These credentials are verified by the entry node, preventing denial-of-service attacks and ensuring that users possess the necessary rights to utilise the Nym network. Zk-nyms provide complete unlinkability between the user's identity or their fiat payment and their activities within the network.

Notably, zk-nyms offer a powerful feature known as selective disclosure. This means users have the control and flexibility to reveal only the information they're comfortable with, enhancing their privacy and security. It ensures that users can access services while disclosing minimal information without leaving a digital paper trail behind.

Zero-knowledge technologies such as zk-nyms are gaining traction across various tech sectors and are notably employed in cryptocurrency projects and the emerging Web3 ecosystem. Thus, zk-nyms fit seamlessly within these developments. For example, in the realm of cryptocurrencies, zk-nyms are an alternative for private transactions without revealing the user's identity or transaction details, adding an essential layer of privacy. In the context of Web3, where decentralisation, privacy, and user empowerment are paramount, zk-nyms play a pivotal role by empowering users to keep personal information in their hands.

4

Comparative Analysis: NymVPN in the Privacy Tools Landscape

In the ever-evolving landscape of online privacy solutions, it's vital to know your options and make informed choices.

NymVPN is not just another player; it's a unique contender in the realm of digital privacy. To help you navigate this dynamic field, we have crafted a side-by-side comparison of NymVPN with similar technologies, highlighting key features, attributes, and differences. This analysis aims to shed light on how the innovations in NymVPN stack up against the alternatives, offering a comprehensive view of the evolving privacy tools landscape.

NymVPN vs Traditional VPNs

In a market where VPNs and network solutions commonly adopt centralised approaches, NymVPN stands out for its steadfast commitment to decentralisation. Key players like IVPN, ProtonVPN, and MullvadVPN manage their nodes centrally, inherently falling short in providing the same level of privacy as their decentralised counterparts, as they retain visibility over user data and browsing history, presenting potential privacy concerns. In contrast, NymVPN champions decentralisation by empowering independent third parties to operate relay nodes, thereby preventing any single entity from correlating users with their online activities, thus safeguarding user privacy.

NymVPN further sets itself apart with default multi-hop routing, a critical privacy feature. While IVPN, ProtonVPN, and MullvadVPN offer multi-hop as an optional feature, their centralised setups limit the benefits of this capability.

Due to their centralised structure, traditional providers such as IVPN, ProtonVPN, and MullvadVPN lack community involvement in decisions concerning the relays within the network. NymVPN, in contrast, fosters community governance through stake delegation and robust feedback mechanisms

	NymVPN	Traditional VPNs
Decentralised	✅	❌
Multi-hop	Default	Optional
Community Governance	✅	❌
Traffic Analysis Resistance	Mixnet mode	❌

NymVPN vs Decentralised VPNs

Over recent years, several decentralised VPN services have been proposed, with Sentinel, Mysterium, and Orchid promoting a similar vision, although with some distinctions. Both Sentinel and Mysterium offer a decentralised network of relay nodes, however, both currently lack support for multi-hop routing, thus making users more vulnerable to activity correlation. On the other hand, Orchid, despite its promise of decentralisation, currently operates its nodes through the company and its partners, deviating from the envisioned community-oriented approach. This hybrid model raises concerns about the degree of decentralisation Orchid offers, and its potential impact on user privacy. Moreover, Mysterium's and Orchid's lack of support for community governance of the relay nodes hinders the collaborative and transparent nature of the network. In contrast to those solutions, NymVPN ensures true decentralisation and default multi-hop routing. Another distinguishing factor between NymVPN and Sentinel, Mysterium, and Orchid is the selection of the payment protocol utilised to incentivise relay nodes.

In the Mysterium network, the payment system relies on the use of MYST tokens and smart contracts to facilitate transactions between consumers and service providers. While this mechanism offers a transparent and secure way to handle payments, it comes with inherent privacy challenges. The recording of all transactions on the Ethereum blockchain poses a significant risk to user privacy, as it allows external parties to trace transactions and monitor account states. Consequently, this visibility compromises the anonymity of users and exposes their interactions with the network, including the identification of specific nodes acting as proxies for particular users, potentially compromising the overall privacy and security of the network.

Orchid utilises a probabilistic nanopayments protocol, functioning as a layer 2 solution, to facilitate payments for the relay operators. The payment mechanism operates on a per-packet basis, facilitating frequent transactions for the exchange of bandwidth. In this setup, users create nanopayment tickets linked to their Orchid Identity, which are then handed off-chain to providers in exchange for services. While some of these tickets are winning tickets, the provider cannot ascertain their status until they are used. However, when a winning ticket is utilised, it generates a public record on the Ethereum blockchain, containing the user's Ethereum address, the provider's Ethereum address, and a timestamp. Consequently, Orchid payments lack complete anonymity, allowing anyone to link the nodes used by the user, even the ones involved in the same circuit. To mitigate privacy risks within multi-hop circuits, Orchid clients are advised to employ different accounts for each hop, although this solution may pose challenges in terms of user convenience.

In contrast, NymVPN's utilisation of zk-nyms technology is integral to ensuring users' zero-knowledge access to the Nym network. These sophisticated cryptographic credentials not only grant access to the network but also serve as secure digital e-cash, facilitating payments for the use of the Nym network's relay nodes. Importantly, zk-nyms guarantee that user privacy remains intact throughout the payment process, as they prevent any information leakage concerning the specific nodes used by the user to route their traffic or the user's activities. This robust system effectively safeguards the user's anonymity and shields their activity from any potential surveillance or tracking.

Moreover, NymVPN's provision of a powerful mixnet mode allows users to fully obfuscate their communication patterns, making it exceedingly difficult for any network observer, even advanced adversaries, to trace their online behaviour. This feature is crucial for those who require an extra layer of protection for their sensitive online activities.

	NymVPN	Sentinel	Mysterium	Orchid
Decentralised	✓	✓	✓	✓
Multi-hop	Default	✗	✗	Optional
Community Governance	✓	✓	✓	✓
Privacy-preserving node rewards	✓	✗	✗	✗
Traffic Analysis Resistance	Mixnet mode	✗	✗	✗

NymVPN vs Tor

When examining the decentralised landscape, Tor, with its renowned onion-routing methodology, remains a prominent player in the privacy domain. However, Tor, relying on volunteers to operate its nodes, lacks essential features such as Sybil attack resistance and incentives for node operators. The absence of incentives might lead to unreliable network performance and a reduced level of commitment from node operators, compromising the network's overall reliability and efficiency. The vulnerability to Sybil attacks, on the other hand, opens the door to malicious actors manipulating the network, leading to compromises of the system's underlying integrity and data breaches, thereby undermining the very core principles of user privacy and network security. Additionally, the absence of community governance mechanisms for the relay nodes within the Tor network limits the active participation of community members in decision-making processes related to the network's operation and policies. This lack of inclusivity could potentially lead to a reduced sense of ownership among network participants and a limited ability to address governance-related issues effectively, ultimately impacting the network's agility and adaptability. Additionally, the absence of community governance mechanisms for the relay nodes within the Tor network, whose list is determined by the semi-centralised directory authorities, limits the active participation of community members in decision-making processes related to the network's operation and policies. On top of that, NymVPN in mixnet mode offers much stronger privacy guarantees than Tor.

By actively reshuffling the packets during transmission, NymVPN effectively thwarts any attempts at packet timing analysis, a vulnerability that exists within the Tor network where packets are forwarded in a strictly first-in-first-out (FIFO) order. Additionally, NymVPN's utilisation of cover traffic injects a strategic blend of dummy packets that mimic a user's normal data flow, thereby obfuscating communication patterns and rendering various traffic analysis attacks futile. This powerful combination of packet shuffling and cover traffic solidifies the mixnet mode as a cutting-edge solution for users seeking the highest level of privacy for their online activities.

	NymVPN	Tor
Decentralised	✅	✅
Multi-hop Routing	✅	✅
Incentivised relay nodes	✅	❌
Sybil attack resistance	✅	❌
Community Governance	✅	❌
Traffic Analysis Resistance	Mixnet mode	❌

NymVPN vs Other Mixnet Design

Understanding the landscape of emerging mix network designs is crucial in fully appreciating the distinct capabilities of NymVPN's mixnet mode. We examine its unique features alongside established mix networks, particularly Elixxir and HOPR, both of which have active deployments, allowing for a comprehensive evaluation of their respective strengths and limitations.

Nym network and Elixxir represent two distinct mix network designs, each employing unique strategies to ensure user privacy and network performance. Nym's utilisation of a layered topology for its nodes stands in contrast to Elixxir's cascade topology. This fundamental distinction has a significant impact on the scalability and latency of the networks. While Elixxir employs a single cascade topology and relies on simple packet batching shuffling techniques, Nym's layered topology facilitates horizontal scalability, enabling the network to seamlessly accommodate an expanding user base without compromising end-to-end latency. Nym's privacy capabilities are further augmented by its unique packet mixing and rearranging technique, with an increased volume of traffic correlating with heightened anonymity. In contrast, Elixxir's fixed-size batching maintains a relatively modest anonymity set of 1,000 packets, limiting its privacy offerings as the network grows. Moreover, the use of a single cascade topology presents challenges to Elixxir when handling larger traffic volumes, potentially leading to latency issues and reduced user privacy as the network expands.

Nym's mixnet mode employs a variant of the Sphinx protocol, a compact and secure packet format specifically optimised for multi-hop networks. This protocol encapsulates all the essential routing information required for secure and anonymous traffic routing within the packet itself. As a result, there is no need for any pre-computations or lengthy preliminary phases for key derivation. This efficient packet format streamlines the processing time, ensuring that packet handling occurs within mere hundreds of nanoseconds, contributing to minimal end-to-end latency overhead and efficient network performance.

On the other hand, Elixxir employs conventional encryption methods, requiring a preliminary phase for key derivation before actual communication, which slows down proportionally with the size of the anonymity set. Additionally, the subsequent communication phase in Elixxir yields notably higher end-to-end latency, often in the order of seconds.

HOPR adopts a distinct path by employing a peer-to-peer architecture for its mix network, where participants function as both relay nodes and end users. Despite its potential for scalability, the network faces a substantial draw-

back in providing adequate anonymity as the user base grows. The sparsely distributed traffic across thousands of links hinders efficient packet shuffling, thereby rendering traffic analysis relatively effortless. This limitation severely undermines the network's objective of offering robust resistance to traffic analysis. Furthermore, unlike our mixnet mode, HOPR lacks robust features for obfuscating user behaviours and communication patterns, resulting in an overall weaker approach to privacy compared to established mixnet designs such as Nym, Elixxir or even onion-routing Tor.

In addition to the architectural limitations, HOPR's use of payment-channel networks for rewarding relay nodes introduces further concerns. While payment-channel networks aim to keep transactions offline, recent research has revealed that they do not ensure adequate privacy for either the users or the nodes involved in packet routing. This inadequacy in ensuring end-to-end privacy within the network heightens the risks associated with potential data compromises, underscoring the fundamental importance of employing robust privacy measures in any mixnet design.

	NymVPN	Elixxir	HOPR
Decentralised	✓	✓	✓
Multi-hop Routing	✓	✓	Optional
Incentivised Relays	✓	✗	✓
Scalable network	✓	✗	✓
Secure and Efficient Enryption Protocol	✓	✗	✓
Community Governance of the Relay Nodes	✓	✗	✗
Robust Resistance to Traffic Analysis	✓	✓	✗
Large Anonymity Set	✓	✗	✗
Multi-App Support	✓	✗	✗

NYM

Web
nymtech.net

Email
info@nymtech.net

Twitter
@nymproject

Github
@nymtech