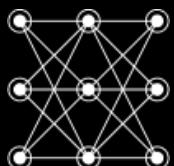


NYM

# NymVPN Litepaper



Protigiendo patrones de comunicación  
para todo el trafico de internet.

# Index

<b>1. Introducción y motivación.....</b>	<b>3</b>
<b>La Necesidad de Privacidad en Línea.....</b>	
Centralización: Un Riesgo para su Privacidad.....	
El Dilema de los Incentivos: ¿Quién se Beneficia?.....	
Navegando un Mar de Soluciones de Privacidad.....	
Las Trampas de los Sistemas de Pago de VPN	
Tradicionales.....	
<b>2. Nuestra solución.....</b>	<b>5</b>
NymVPN: Una puerta a la privacidad en línea .....	
Acceso a la red Nym verdaderamente descentralizada .....	
Privacidad racionalizada en una solución unificada .....	
Control total y privacidad inigualable en todos los dispositivos .....	
Cifrado seguro y de vanguardia en su núcleo .....	
Solución multihop .....	
Acceso sin fronteras .....	
Protección de la intimidad con pagos imposibles de rastrear y acceso .....	
<b>3. Panorama técnico .....</b>	<b>8</b>
Arquitectura de la red Nym.....	
Dos modos para mejorar la privacidad: dVPN y Mixnet .....	
Desbloqueo de la privacidad en diversos ámbitos digitales .....	
Sus datos, sus reglas: Dominar la privacidad con credenciales de Zero Knowledge .....	
<b>4. Análisis comparativo: NymVPN en el panorama de las herramientas de privacidad ..</b>	<b>12</b>
NymVPN vs VPNs tradicionales .....	
Nym VPN vs VPNs Descentralizadas .....	
Nym VPN vs Tor .....	
Nym VPN vs Otras mixnets diseñadas .....	

# 1

# Introducción y Motivación

**En una época en la que nuestras vidas están cada vez más entrelazadas con el ámbito digital, salvaguardar la privacidad en línea se ha convertido en un imperativo.**

El rápido aumento de las violaciones de datos, los ciberataques, la vigilancia generalizada y el geobloqueo ha puesto de relieve la necesidad de herramientas sólidas que permitan a las personas recuperar su privacidad, proteger su huella digital y recuperar el acceso sin restricciones al mundo en línea. Por estas razones, ahora es el momento de presentar la aplicación NymVPN, una plataforma revolucionaria que ofrece a los usuarios acceso a una VPN descentralizada y a una mixnet descentralizada en una única aplicación, proporcionando el máximo nivel de privacidad y seguridad para sus actividades en línea.

## La necesidad de privacidad en línea

El panorama digital está plagado de amenazas, desde cibercriminales que buscan explotar vulnerabilidades hasta entidades de vigilancia que acaparan datos personales sin consentimiento. Además, las restricciones gubernamentales y la censura en línea en varias regiones no solo ahogan el libre intercambio de ideas, sino que también dificultan el acceso a información vital. La privacidad del usuario no es un mero lujo, sino un escudo esencial contra la usurpación de identidad, el rastreo intrusivo y la erosión de nuestro derecho fundamental a acceder a la información y expresarnos libremente en la era digital.

El cifrado o las transmisiones seguras no bastan por sí solos para salvaguardar la privacidad en línea. La protección de los metadatos -los datos sobre sus datos- sigue siendo un reto formidable. Los metadatos pueden revelar mucho sobre su comportamiento en línea, sus relaciones e incluso su estado de ánimo, dejándole expuesto a un posible seguimiento y vigilancia. La mayoría de las tecnologías existentes se quedan cortas a la hora de proteger los metadatos, lo que deja una laguna crítica en las defensas de su privacidad.

## Centralización: Un riesgo para su intimidad

En la era digital, las soluciones centralizadas se han convertido en la norma. Sin embargo, esto tiene un coste en términos de privacidad y seguridad. Las VPN tradicionales conocen tu identidad y tu historial de navegación. Por lo tanto, confiar tu privacidad online a una entidad centralizada te expone a un único punto de control, dejando tus datos expuestos a posibles violaciones, recolección y vigilancia. Entregar esta confianza a una sola empresa crea un único punto de fallo y deja sus datos vulnerables a las violaciones y la vigilancia. La necesidad de una alternativa descentralizada se hace evidente con la creciente frecuencia de las violaciones de datos y los ciberataques.

## **El dilema de los incentivos: ¿a quién beneficia?**

En un mundo en el que los datos son poder, incentivar a las personas para que participen activamente en la protección de la privacidad digital se convierte en algo primordial. Las redes multihop tradicionales carecen a menudo de mecanismos para recompensar la participación en la red, lo que desmotiva a los operadores de los nodos. Este vacío puede crear un entorno en el que la calidad y la fiabilidad de los nodos de la red son inconsistentes, y los intereses de los usuarios pueden no ser la principal preocupación. Los servicios VPN gratuitos, en particular, a menudo extraen el coste de su servicio "gratuito" de la privacidad de los usuarios y venden la actividad de los usuarios a intermediarios de datos. Además, incluso en el caso de Tor, que es una herramienta valiosa para las comunicaciones privadas, la calidad del servicio varía porque los operadores no están incentivados para ofrecer un servicio coherente y fiable, sino que la red se basa en la buena voluntad.

## **Navegar por un mar de soluciones de privacidad**

En el panorama digital actual, los usuarios se enfrentan a un enigma desconcertante en lo que respecta a la privacidad. Diversas herramientas de privacidad ofrecen distintos niveles de protección, lo que las hace adecuadas para distintos casos de uso. Por ejemplo, las VPN suelen ser las preferidas para una navegación segura, mientras que el enrutamiento cebolla y las redes mixtas son alabadas por sus funciones de anonimato. Sin embargo, los usuarios suelen tener que hacer malabarismos con varias aplicaciones, cada una adaptada a un fin específico. Esta complejidad crea un enfoque fragmentado de la privacidad y obliga a las personas a cambiar de aplicación en función de sus necesidades de uso. Además, los usuarios no suelen tener un conocimiento claro de las propiedades específicas de privacidad que ofrecen los distintos sistemas. Los entresijos de los protocolos de cifrado, los métodos de enrutamiento y las prácticas de gestión de datos pueden resultar desalentadores, por lo que muchos usuarios no saben qué herramienta elegir para sus necesidades específicas. Como resultado, tomar una decisión informada sobre cómo proteger su vida digital se convierte en una ardua batalla.

## **Los problemas de los sistemas tradicionales de pago VPN**

En el panorama tradicional de los servicios VPN, las transacciones de pago se interconectan de forma rutinaria con las actividades en línea del usuario, dando lugar a un rastro de datos que pueden rastrearse hasta su huella digital. Esta vinculación plantea un riesgo crítico para la privacidad, ya que no sólo compromete el anonimato de los usuarios, sino que también abre la puerta a que terceros puedan conectar potencialmente la identidad de un usuario con su historial específico de navegación y sus patrones de uso de Internet. Las implicaciones de esta visibilidad son de gran alcance y a menudo dan lugar a la violación de la intimidad, la vigilancia injustificada y la elaboración de perfiles específicos. La exposición de esta información sensible deja a los usuarios expuestos a una serie de riesgos de seguridad, como la usurpación de identidad, la extracción de datos y la publicidad invasiva, lo que socava fundamentalmente la privacidad y la seguridad en línea. En consecuencia, existe una necesidad urgente de una solución de pago más sólida y que preserve la privacidad, que garantice que la identidad del usuario no está conectada a sus actividades en línea, preservando su autonomía digital.

# 2

## Nuestra solución

**En una era en la que el panorama digital está plagado de problemas de privacidad y vulnerabilidad de los datos, NymVPN emerge como un faro de privacidad y seguridad en línea.**

NymVPN es su compañero de confianza en la era digital, diseñado para dar respuesta a los apremiantes retos a los que se enfrentan los usuarios que buscan salvaguardar su información personal, mantener su autonomía digital y navegar por Internet sin compromisos.

Con la aplicación NymVPN, ofrecemos una solución robusta que combina el poder de una VPN descentralizada y una mixnet descentralizada, marcando el comienzo de una nueva era de protección de la privacidad en línea. NymVPN garantiza que su huella digital permanezca segura y que sus actividades en línea sean realmente privadas.

### **NymVPN: Su puerta a la privacidad en línea**

NymVPN ofrece una seguridad en línea sin igual. Al combinar el cifrado y la protección de metadatos, NymVPN es la piedra angular de nuestro compromiso para garantizar la privacidad digital, la seguridad, la integridad y la autonomía.

Con NymVPN, usted obtiene acceso a la red Nym, una revolucionaria red descentralizada de nodos gestionados por individuos, no por autoridades centrales. Esta red es el epítome de la verdadera descentralización, donde cualquiera puede gestionar un nodo, fomentando un ecosistema diverso. Este enfoque garantiza que ninguna entidad pueda poner en peligro tu privacidad. La fuerza de la red Nym reside en sus operadores de nodos dedicados, que son recompensados por su fiabilidad y servicio fiable. Gracias al token NYM, estos incentivos alinean los intereses de los operadores con los objetivos de seguridad y privacidad de la comunidad.

Nuestro exclusivo mecanismo de delegación ofrece a los titulares de tokens NYM la libertad de apostar sus tokens a operadores de nodos en los que confíen. Este proceso de delegación democrática también sirve como sistema de reputación impermeable y como defensa contra los ataques Sybils. Intentar comprometer la integridad de la red mediante este tipo de tácticas es arduo e inútil, gracias al sistema de delegación transparente y democrático. Por su participación e implicación en garantizar la integridad de la red, los delegados también reciben una parte de las recompensas de los nodos.

Con más de 600 nodos sirviendo activamente a usuarios en casi 60 países, la red Nym es un sistema descentralizado práctico, global y escalable. Tanto si el usuario elige el modo dVPN como mixnet, NymVPN garantiza que las interacciones digitales sean privadas y seguras gracias a las potentes capacidades de protección de la red Nym.

## **Privacidad optimizada en una solución unificada**

En el mundo digital actual, los usuarios se ven obligados a elegir entre un abanico de soluciones fragmentadas para conseguir privacidad. En cambio, NymVPN es un ejemplo de simplicidad, ya que aúna una dVPN y una mixnet en una aplicación sin fisuras, todas ellas alimentadas por la misma red subyacente. La elección depende del usuario: tanto si necesita una dVPN multihop para la navegación diaria como el anonimato total de una mixnet, NymVPN es una única solución integrada. Con NymVPN, la privacidad es una experiencia unificada que simplifica el acceso a una vida digital más segura.

## **Control total y privacidad inigualable en todos los dispositivos**

NymVPN ofrece privacidad sin concesiones en todos sus dispositivos con su fiable servicio de protección de red completa, protegiendo cada interacción en línea. Lo que distingue a NymVPN es su capacidad para adaptar automáticamente las funciones de privacidad a cada caso de uso único, aprovechando una combinación única de tecnologías mixnet y WireGuard VPN de última generación. A diferencia de las VPN tradicionales, NymVPN no limita las protecciones a SOCKS5, sino que cubre toda la conectividad a la red, mientras que un interruptor de corte integrado proporciona salvaguardas adicionales en caso de que se caiga la conexión. Con la tunelización dividida, NymVPN permite a los usuarios elegir si el tráfico de aplicaciones se dirige a través de la dVPN o de la mixnet, mientras que las configuraciones granulares suponen un mayor control del usuario sobre las preferencias de privacidad. Toda esta potencia y comodidad se integran en una sola aplicación, ofreciendo una solución integral para todas las necesidades de conectividad de red. Con NymVPN, su privacidad en línea no es sólo una característica, es una garantía.

## **Cifrado avanzado y seguro en su núcleo**

NymVPN protege su tráfico de Internet de miradas indiscretas con un cifrado indescifrable que incluye AES-256, ChaChaPo- ly y Lioness. Tanto si comparte información confidencial, realiza operaciones bancarias en línea o simplemente navega por Internet, sus datos estarán perfectamente protegidos y fuera del alcance de ciberdelincuentes y entidades de vigilancia en línea. Este manto digital protege su información personal y confidencial, protegiéndole de las escuchas clandestinas, las violaciones de datos y el robo de identidad.

Además, estamos comprometidos con el futuro de la seguridad en línea. Aunque nuestros estándares de cifrado ya son extremadamente sólidos, aspiramos a que sean seguros post-cuánticos, adelantándonos a las amenazas emergentes y garantizando la privacidad digital incluso ante la evolución de la tecnología.

## **Solución multihop**

Además de la encriptación, NymVPN emplea una arquitectura multihop que protege su identidad digital del rastreo de la red y mejora su seguridad. En lugar de enrutar el tráfico a través de un único nodo proxy como la mayoría de las VPN, Nym-VPN da un paso más y enruta el tráfico a través de dos nodos proxy independientes en el modo VPN, o cinco nodos en el modo mixnet - frustrando los ataques man-in-the-middle y asegurando que los nodos individuales en la ruta no puedan vincular al usuario con sus actividades digitales.

Este enfoque multihop añade una capa adicional de privacidad, haciendo mucho más difícil para los sitios web, los anunciantes y los actores maliciosos rastrear su comportamiento en línea. Su identidad en línea queda salvaguardada, lo que garantiza la protección de su privacidad digital.

## **Acceso sin fronteras**

NymVPN es más que una herramienta para la privacidad en línea; es un compromiso con un futuro en el que la libertad en línea no conoce fronteras. Aunque nuestra versión actual ofrece soluciones de privacidad sólidas, somos conscientes de que la lucha por una Internet verdaderamente abierta no termina aquí. Nos dedicamos a mejorar e integrar continuamente técnicas novedosas y probadas que refuerzan la resistencia de NymVPN a los mecanismos de censura.

Nuestro objetivo es empoderar a las personas de todo el mundo, asegurando que tengan acceso sin restricciones a la información y los recursos que buscan. A medida que evoluciona el panorama digital, NymVPN evolucionará con él, desarrollando e implementando activamente métodos innovadores para eludir la censura y salvaguardar su libertad en línea.

## **Proteger la intimidad con pagos y accesos imposibles de rastrear**

NymVPN aborda los desafíos críticos relativos a la privacidad de los pagos, garantizando que los usuarios puedan acceder a nuestros servicios mientras salvaguardan su identidad digital. Nuestra innovadora tecnología zk-nyms ofrece un escudo sin precedentes de conocimiento cero de las transacciones en cualquier moneda o criptomoneda para pagar por el servicio, evitando cualquier correlación entre la identidad del usuario o la información de pago y los sitios web o servicios específicos a los que se accede dentro de la red Nym. Por ejemplo, el pago incluso en Bitcoin podría desanonomizar a los usuarios al estar vinculado a su acceso a NymVPN, pero los zk-nyms convierten cualquier pago en NYM y proporcionan un "comprobante de pago" no vinculable en zero knowledge. Con los zk-nyms, el pago de los servicios NymVPN garantiza que ni los operadores de nodos ni ninguna entidad externa puedan vincular la identidad del usuario con los sitios web o servicios que utiliza.

# 3

## Resumen técnico

**NymVPN capacita a los usuarios proporcionándoles acceso activo a la red Nym, un sólido sistema diseñado para proteger su privacidad en línea.**

### Arquitectura de la red Nym

La red Nym es un ecosistema descentralizado formado por varias entidades clave, cada una de las cuales desempeña un papel vital a la hora de garantizar la privacidad y la seguridad de las actividades de los usuarios.

#### **Nodos de retransmisión:**

Estos nodos forman la columna vertebral de la red Nym. Se encargan de encaminar el tráfico de Internet de los usuarios a través de rutas multihop, añadiendo capas de privacidad y seguridad a las actividades en línea. Los nodos de retransmisión son gestionados por personas independientes, cada una de las cuales contribuye a la potente descentralización de la red.

#### **Validadores:**

Estos validadores desempeñan un papel fundamental en el mantenimiento de la blockchain Nym, sirviendo no sólo como un canal de difusión seguro para la distribución de información crítica en toda la red, sino también como una infraestructura de clave pública descentralizada. Además, los validadores se encargan de distribuir las recompensas a los operadores de los nodos, garantizando así la correcta incentivación de los participantes en la red.

#### **Nodos Nym-API:**

Los nodos Nym-API tienen un papel diferenciado dentro de la red. Son los responsables de emitir las credenciales zk-nym, un componente crítico del acceso de los usuarios a la red Nym. Estas credenciales sirven como comprobante de pago de las suscripciones de los usuarios y son esenciales para garantizar la participación en la red.

Juntas, estas entidades forman un entorno descentralizado y privado en el que los usuarios pueden disfrutar de actividades en línea sin comprometer sus datos personales ni su seguridad.

## Dos modos para mejorar la privacidad: dVPN y Mixnet

### Modo VPN: El poder de Wireguard y la novedosa encriptación Onion

NymVPN le ofrece dos modos distintos para salvaguardar sus actividades en línea: la dVPN y la mixnet. En el modo dVPN, sus datos atraviesan una ruta segura de 2 hops, cada uno de ellos alojado por un operador independiente. Esta configuración combina el fiable protocolo Wireguard, conocido por su cifrado de alto rendimiento, con un novedoso esquema de cifrado por capas. Nuestra elección de Wireguard garantiza una seguridad y velocidad excepcionales, lo que lo convierte en la opción ideal para proteger sus datos al tiempo que se optimiza la velocidad. El novedoso esquema de cifrado por capas, garantiza la confidencialidad e integridad de los datos y proporciona una capa adicional de seguridad, impidiendo que los nodos individuales que enrutan la conexión correlacionen al usuario con su actividad en línea. Además, emplea el relleno de paquetes para garantizar la uniformidad del tamaño de los mismos, lo que añade una capa adicional de seguridad.

Por lo tanto, el modo dVPN proporciona una solución de acceso en línea rápida y de alta velocidad, perfecta para actividades como la navegación web, los juegos y el streaming. Es excelente a la hora de ocultar tu dirección IP a los servidores web y garantiza que no haya ningún punto de control centralizado, gracias a su estructura independiente de 2 hops.

Aunque el modo dVPN ofrece fuertes medidas de privacidad, es importante señalar que no ofrece el mismo nivel de resistencia contra los ataques avanzados de análisis de tráfico empleados por adversarios sofisticados de la red.

### Modo Mixnet: Privacidad avanzada y protección de metadatos

Para los casos de uso en los que los usuarios buscan protecciones de privacidad completas, el modo mixnet de NymVPN ofrece una seguridad sólida y lleva la privacidad de los usuarios al siguiente nivel al ofrecer resistencia al análisis del tráfico. En este modo, sus datos viajan a través de una ruta segura de 5 hops, en la que cada hop introduce una capa adicional de protección. Para ocultar sus patrones de comunicación, se genera tráfico encubierto, inyectando paquetes ficticios que no se distinguen de su tráfico normal. Lo que distingue a este modo es el barajado avanzado de paquetes que realizan los tres nodos internos en la ruta de 5 hops. Este proceso garantiza que los paquetes no puedan correlacionarse en función de su temporización, lo que aumenta significativamente la privacidad. Como resultado, el modo mixnet proporciona una seguridad sin precedentes, incluso frente a sofisticados ataques de análisis de tráfico. Incluso en presencia de observadores de red globales o ataques avanzados de aprendizaje automático, este modo garantiza que sus actividades en línea sigan siendo confidenciales y estén protegidas de miradas indiscretas. Así, supera las propiedades de privacidad de las VPN tradicionales y Tor y es el mixnet más rápido y seguro disponible hoy en día, manteniendo tus actividades en línea verdaderamente privadas.

Aunque la ruta de 5 hops y las medidas de seguridad adicionales introducen una latencia de comunicación mayor en comparación con el modo dVPN, el modo mixnet es una opción ideal para aplicaciones que priorizan la privacidad sobre la baja latencia, como el envío de transacciones de criptomonedas, la mensajería segura, los correos electrónicos confidenciales o el intercambio de archivos confidenciales.

## **Mejorar la privacidad mediante una red unificada**

Al enrutar los modos dVPN y mixnet a través de la misma red subyacente, NymVPN ofrece una capa adicional de privacidad y seguridad. Este enfoque garantiza que los observadores de la red no puedan diferenciar entre el tráfico dVPN y mixnet dentro de la red, ofuscando eficazmente el flujo de datos. Este enfoque integrado mejora la privacidad del usuario añadiendo complejidad para cualquier entidad que intente vigilar las actividades en línea.

## **Desbloquear la privacidad en diversos ámbitos digitales**

NymVPN va más allá de la seguridad de la navegación web, ya que ofrece compatibilidad con una amplia gama de aplicaciones y servicios. Los usuarios pueden configurar aplicaciones de mensajería instantánea (IM) y chat para conectarse a la red Nym a través de la aplicación NymVPN, garantizando la confidencialidad de sus conversaciones privadas. Del mismo modo, los clientes de correo electrónico pueden configurarse para enrutar el tráfico a través de NymVPN, proporcionando a los usuarios una forma segura y anónima de acceder y enviar correos electrónicos. Para los entusiastas de las criptodivisas, NymVPN ofrece la opción de conectar monederos de criptodivisas, lo que evita el rastreo de direcciones de monederos y del historial de transacciones. Esta amplia compatibilidad garantiza que los usuarios puedan disfrutar de las ventajas de una mayor privacidad en diversas plataformas y servicios en línea.

En su versión actual, los usuarios pueden configurar cualquier aplicación, siempre que sea compatible con SOCKS5, para conectarse a la red Nym a través de la aplicación NymVPN. Mirando hacia el futuro, NymVPN está a las puertas de un desarrollo emocionante. En un futuro cercano, NymVPN ampliará esta capacidad para trabajar con cualquier tráfico IP (ICMP, TCP, UDP) desde cualquier aplicación.

## **Sus datos, sus reglas: Dominar la privacidad con credenciales de Zero Knowledge**

NymVPN utiliza nuestras credenciales anónimas de conocimiento cero llamadas zk-nyms. Este sofisticado protocolo criptográfico combina la potencia de la tecnología de Zero Knowledge las firmas digitales para conceder a los usuarios acceso a la red Nym y a sus servicios sin necesidad de revelar ninguna información sensible sobre su identidad. Cuando los usuarios optan por una suscripción y efectúan el pago en fiat, nuestro sistema transforma el pago en una orden de compra en el mercado abierto de NYM. A continuación, nuestro innovador sistema de pago intercambia rápidamente los NYM por credenciales zk-nyms, que actúan como una especie de "comprobante de pago NYM" digital para transacciones seguras y privadas en la red Nym. Estas credenciales son verificadas por el nodo de entrada, evitando ataques de denegación de servicio y garantizando que los usuarios poseen los derechos necesarios para utilizar la red Nym. Los Zk-nyms proporcionan una total desvinculación entre la identidad del usuario o su pago en fiat y sus actividades dentro de la red.

En particular, zk-nyms ofrece una potente función conocida como revelación selectiva. Esto significa que los usuarios tienen el control y la flexibilidad para revelar sólo la información con la que se sienten cómodos, mejorando su privacidad y seguridad. Garantiza que los usuarios puedan acceder a los servicios revelando un mínimo de información sin dejar un rastro de papel digital.

Las tecnologías de conocimiento cero, como los zk-nyms, están ganando terreno en diversos sectores tecnológicos y se emplean sobre todo en proyectos de criptomoneda y en el emergente ecosistema Web3. Por tanto, los zk-nyms encajan perfectamente en estos desarrollos. Por ejemplo, en el ámbito de las criptomonedas, los zk-nyms son una alternativa para realizar transacciones privadas sin revelar la identidad del usuario ni los detalles de la transacción, lo que añade una capa esencial de privacidad. En el contexto de la Web3, donde la descentralización, la privacidad y el empoderamiento del usuario son primordiales, los zk-nyms desempeñan un papel fundamental al permitir a los usuarios mantener su información personal en sus manos.

# 4

## Análisis comparativo: NymVPN en el panorama de las herramientas de privacidad

**En el panorama en constante evolución de las soluciones para la privacidad en línea, es fundamental conocer las opciones y elegir con conocimiento de causa.**

NymVPN no es un jugador más; es un contendiente único en el ámbito de la privacidad digital. Para ayudarle a navegar por este dinámico campo, hemos elaborado una comparación de NymVPN con tecnologías similares, destacando las características, atributos y diferencias clave. Este análisis pretende arrojar luz sobre cómo las innovaciones de NymVPN se comparan con las alternativas, ofreciendo una visión completa del panorama de las herramientas de privacidad en evolución.

### **NymVPN vs las VPNs tradicionales**

En un mercado en el que las VPN y las soluciones de red suelen adoptar enfoques centralizados, NymVPN destaca por su firme compromiso con la descentralización. Los principales actores, como IVPN, ProtonVPN y MullvadVPN, gestionan sus nodos de forma centralizada, por lo que no ofrecen el mismo nivel de privacidad que sus homólogos descentralizados, ya que conservan la visibilidad de los datos del usuario y el historial de navegación, lo que puede plantear problemas de privacidad. En cambio, NymVPN aboga por la descentralización al permitir que terceros independientes gestionen los nodos de retransmisión, lo que impide que una única entidad correlacione a los usuarios con sus actividades en línea, salvaguardando así su privacidad.

NymVPN se distingue además por su enrutamiento multihop por defecto, una función de privacidad fundamental. Mientras que IVPN, ProtonVPN y MullvadVPN ofrecen multihop como función opcional, sus configuraciones centralizadas limitan las ventajas de esta capacidad.

Debido a su estructura centralizada, los proveedores tradicionales como IVPN, ProtonVPN y MullvadVPN carecen de participación comunitaria en las decisiones relativas a los repetidores de la red. NymVPN, en cambio, fomenta el gobierno de la comunidad mediante la delegación de responsabilidades y sólidos mecanismos de retroalimentación.

En particular, zk-nyms ofrece una potente función conocida como revelación selectiva. Esto significa que los usuarios tienen el control y la flexibilidad para revelar sólo la información con la que se sienten cómodos, mejorando su privacidad y seguridad. Garantiza que los usuarios puedan acceder a los servicios revelando un mínimo de información sin dejar un rastro de papel digital.

Las tecnologías de conocimiento cero, como los zk-nyms, están ganando terreno en diversos sectores tecnológicos y se emplean sobre todo en proyectos de criptomoneda y en el emergente ecosistema Web3. Por tanto, los zk-nyms encajan perfectamente en estos desarrollos. Por ejemplo, en el ámbito de las criptomonedas, los zk-nyms son una alternativa para realizar transacciones privadas sin revelar la identidad del usuario ni los detalles de la transacción, lo que añade una capa esencial de privacidad. En el contexto de la Web3, donde la descentralización, la privacidad y el empoderamiento del usuario son primordiales, los zk-nyms desempeñan un papel fundamental al permitir a los usuarios mantener su información personal en sus manos.

	<b>NYM VPN</b>	<b>VPN TRADICIONALES</b>
<b>Descentralizado</b>	✓	✗
<b>Multihop</b>	Por Defecto	Opcional
<b>Gobernanza Comunitaria</b>	✓	✗
<b>Resistencia al análisis del tráfico</b>	Modo Mixnet	✗

## NymVPN frente a VPN descentralizadas

En los últimos años, se han propuesto varios servicios VPN descentralizados. Sentinel, Mysterium y Orchid promueven una visión similar, aunque con algunas diferencias. Tanto Sentinel como Mysterium ofrecen una red descentralizada de nodos de retransmisión, pero ambos carecen actualmente de soporte para enrutamiento multihop, lo que hace a los usuarios más vulnerables a la correlación de actividades. Por otro lado, Orchid, a pesar de su promesa de descentralización, opera actualmente sus nodos a través de la empresa y sus socios, desviándose del enfoque previsto orientado a la comunidad. Este modelo híbrido suscita dudas sobre el grado de descentralización que ofrece Orchid y su posible impacto en la privacidad de los usuarios. Además, la falta de apoyo de Mysterium y Orchid a la gobernanza comunitaria de los nodos de retransmisión dificulta la naturaleza colaborativa y transparente de la red. A diferencia de estas soluciones, NymVPN garantiza una verdadera descentralización y un encaminamiento multihop por defecto. Otro factor distintivo entre NymVPN y Sentinel, Mysterium y Orchid es la selección del protocolo de pago utilizado para incentivar a los nodos de retransmisión.

En la red Mysterium, el sistema de pagos se basa en el uso de tokens MYST y contratos inteligentes para facilitar las transacciones entre consumidores y proveedores de servicios. Aunque este mecanismo ofrece una forma transparente y segura de gestionar los pagos, conlleva problemas de privacidad inherentes. El registro de todas las transacciones en la blockchain de Ethereum plantea un riesgo significativo para la privacidad del usuario, ya que permite a partes externas rastrear las transacciones y supervisar los estados de cuenta. En consecuencia, esta visibilidad compromete el anonimato de los usuarios y expone sus interacciones con la red, incluida la identificación de nodos específicos que actúan como proxies de usuarios concretos, lo que puede comprometer la privacidad y seguridad generales de la red.

Orchid utiliza un protocolo probabilístico de nanopagos, que funciona como una solución de capa 2, para facilitar los pagos a los operadores de retransmisión. El mecanismo de pago funciona por paquetes, lo que facilita las transacciones frecuentes para el intercambio de ancho de banda. En esta configuración, los usuarios crean boletos de nanopago vinculados a su identidad Orchid, que luego se entregan fuera de la cadena a los proveedores a cambio de servicios. Aunque algunos de estos tickets son ganadores, el proveedor no puede determinar su estado hasta que se utilizan. Sin embargo, cuando se utiliza un boleto ganador, se genera un registro público en la blockchain Ethereum, que contiene la dirección Ethereum del usuario, la dirección Ethereum del proveedor y una marca de tiempo. En consecuencia, los pagos Orchid carecen de anonimato completo, permitiendo que cualquiera pueda vincular los nodos utilizados por el usuario, incluso los que participan en el mismo circuito. Para mitigar los riesgos de privacidad en los circuitos de varios hops, se aconseja a los clientes de Orchid que empleen cuentas diferentes para cada hop, aunque esta solución puede plantear problemas en cuanto a la comodidad del usuario.

En cambio, la utilización de la tecnología zk-nyms por parte de NymVPN es esencial para garantizar a los usuarios un acceso sin conocimiento a la red Nym. Estas sofisticadas credenciales criptográficas no sólo conceden acceso a la red, sino que también sirven como dinero electrónico digital seguro, facilitando los pagos por el uso de los nodos de retransmisión de la red Nym. Y lo que es más importante, los zk-nyms garantizan que la privacidad del usuario permanezca intacta durante todo el proceso de pago, ya que impiden cualquier filtración de información relativa a los nodos concretos utilizados por el usuario para encaminar su tráfico o a las actividades del usuario. Este sólido sistema salvaguarda eficazmente el anonimato del usuario y protege su actividad de cualquier posible vigilancia o rastreo.

Además, NymVPN ofrece un potente modo mixnet que permite a los usuarios ocultar completamente sus patrones de comunicación, lo que dificulta enormemente a cualquier observador de la red (incluso a adversarios avanzados) rastrear su comportamiento en línea.

	NYM VPN	SENTINEL	MYSTERIUM	ORCHID
<b>Descentralizado</b>	✓	✓	✓	✓
<b>Multihop</b>	Por Defecto	✗	✗	Opcional
<b>Gobernanza Comunitaria</b>	✓	✓	✓	✓
<b>Resistencia al análisis del tráfico</b>	Modo Mixnet	✗	✗	✗

## NymVPN vs Tor

Al examinar el panorama descentralizado, Tor, con su famosa metodología de enrutamiento cebolla, sigue siendo un actor prometedor en el ámbito de la privacidad. Sin embargo, Tor, al depender de voluntarios para operar sus nodos, carece de características esenciales como la resistencia a ataques Sybils e incentivos para los operadores de nodos. La ausencia de incentivos podría llevar a un rendimiento poco fiable de la red y a un nivel reducido de compromiso por parte de los operadores de nodos, comprometiendo la fiabilidad y eficiencia general de la red. Por otra parte, la vulnerabilidad a los ataques sibilinos abre la puerta a la manipulación de la red por parte de agentes malintencionados, lo que puede comprometer la integridad subyacente del sistema y la seguridad de los datos, socavando así los principios básicos de la privacidad del usuario y la seguridad de la red. Además, la ausencia de mecanismos de gobierno comunitario para los nodos de retransmisión dentro de la red Tor limita la participación activa de los miembros de la comunidad en los procesos de toma de decisiones relacionados con el funcionamiento y las políticas de la red. Esta falta de inclusión podría llevar potencialmente a un sentido reducido de propiedad entre los participantes de la red y a una capacidad limitada para abordar eficazmente los asuntos relacionados con la gobernanza, impactando en última instancia en la agilidad y adaptabilidad de la red.

Además, la ausencia de mecanismos de gobierno comunitario para los nodos de retransmisión dentro de la red Tor, cuya lista está determinada por las autoridades de directorio semicentralizadas, limita la participación activa de los miembros de la comunidad en los procesos de toma de decisiones relacionados con el funcionamiento y las políticas de la red. Además, NymVPN en modo mixnet ofrece garantías de privacidad mucho más sólidas que Tor.

Al reorganizar activamente los paquetes durante la transmisión, NymVPN frustra eficazmente cualquier intento de análisis de sincronización de paquetes, una vulnerabilidad que existe en la red Tor, donde los paquetes se reenvían siguiendo estrictamente el orden FIFO (primero en entrar, primero en salir). Además, la utilización de NymVPN de tráfico encubierto inyecta una mezcla estratégica de paquetes falsos que imitan el flujo de datos normal de un usuario, ofuscando así los patrones de comunicación y haciendo inútiles varios ataques de análisis de tráfico.

Esta potente combinación de barajado de paquetes y tráfico encubierto consolida el modo mixnet como una solución de vanguardia para los usuarios que buscan el máximo nivel de privacidad para sus actividades en línea.

	NYM VPN	TOR
Descentralizado	✓	✓
Enrutamiento multihop	✓	✗
Resistencia a los ataques sibilinos	✓	✗
Resistencia a los ataques sibilinos	✓	✗
Gobernanza comunitaria	✓	✗
Resistencia al análisis del tráfico	Modo Mixnet	✗

## NymVPN frente a otro diseño de Mixnet

Comprender el panorama de los diseños de redes mixtas emergentes es crucial para apreciar plenamente las capacidades distintivas del modo mixnet de NymVPN. Examinamos sus características únicas junto con las redes mixtas establecidas, en particular Elixxir y HOPR, ambas con despliegues activos, lo que permite una evaluación exhaustiva de sus respectivos puntos fuertes y limitaciones.

La red Nym y Elixxir representan dos diseños de mixnets distintas, cada uno de los cuales emplea estrategias únicas para garantizar la privacidad del usuario y el rendimiento de la red. La utilización por Nym de una topología en capas para sus nodos contrasta con la topología en cascada de Elixxir.

Esta distinción fundamental tiene un impacto significativo en la escalabilidad y latencia de las redes. Mientras que Elixxir emplea una única topología en cascada y se basa en simples técnicas de barajado de paquetes por lotes, la topología en capas de Nym facilita la escalabilidad horizontal, lo que permite a la red acomodar sin problemas una base de usuarios en expansión sin comprometer la latencia de extremo a extremo. La capacidad de privacidad de Nym aumenta aún más gracias a su exclusiva técnica de mezcla y reordenación de paquetes, con un mayor volumen de tráfico correlacionado con un mayor anonimato. Por el contrario, la mezcla de tamaño fijo de Elixxir mantiene un conjunto de anonimato relativamente modesto de 1.000 paquetes, lo que limita su oferta de privacidad a medida que crece la red. Además, el uso de una única topología en cascada plantea problemas a Elixxir a la hora de gestionar grandes volúmenes de tráfico, lo que puede provocar problemas de latencia y reducir la privacidad de los usuarios a medida que crece la red.

El modo mixnet de Nym emplea una variante del protocolo Sphinx, un formato de paquete compacto y seguro optimizado específicamente para redes multihop. Este protocolo encapsula en el propio paquete toda la información de encaminamiento esencial necesaria para el encaminamiento de tráfico seguro y anónimo. Como resultado, no hay necesidad de ningún cálculo previo ni de largas fases preliminares para la derivación de claves. Este eficaz formato de paquete agiliza el tiempo de procesamiento, garantizando que la gestión del paquete se produzca en apenas cientos de nanosegundos, lo que contribuye a una mínima sobrecarga de latencia de extremo a extremo y a un rendimiento eficaz de la red.

Por otra parte, Elixxir emplea métodos de cifrado convencionales, que requieren una fase preliminar para la derivación de claves antes de la comunicación real, que se ralentiza proporcionalmente con el tamaño del conjunto de anonimato. Además, la fase de comunicación posterior en Elixxir produce una latencia de extremo a extremo notablemente mayor, a menudo del orden de segundos.

HOPR adopta una vía distinta al emplear una arquitectura de igual a igual para su mixnet, en la que los participantes funcionan como nodos de retransmisión y usuarios finales. A pesar de su potencial de escalabilidad, la red se enfrenta a un importante drawback a la hora de proporcionar un anonimato adecuado a medida que crece la base de usuarios. El tráfico escasamente distribuido a través de miles de enlaces dificulta el barajado eficaz de paquetes, lo que hace que el análisis del tráfico resulte relativamente sencillo. Esta limitación socava gravemente el objetivo de la red de ofrecer una resistencia robusta al análisis del tráfico. Además, a diferencia de nuestro modo mixnet, HOPR carece de características sólidas para ofuscar los comportamientos de los usuarios y los patrones de comunicación, lo que resulta en un enfoque general más débil a la privacidad en comparación con los diseños mixnet establecidos como Nym, Elixxir o incluso Tor. Además de las limitaciones arquitectónicas,

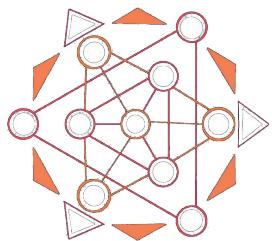
el uso por parte de HOPR de redes de canales de pago para recompensar a los nodos de retransmisión plantea otros problemas. Aunque las redes de canales de pago pretenden mantener las transacciones fuera de línea, investigaciones recientes han revelado que no garantizan la privacidad adecuada ni para los usuarios ni para los nodos implicados en el enrutamiento de paquetes. Esta insuficiencia para garantizar la privacidad de extremo a extremo dentro de la red aumenta los riesgos asociados a las posibles promesas de datos, lo que subraya la importancia fundamental de emplear medidas de privacidad sólidas en cualquier diseño de mixnet.

	NYM VPN	ELIXXIR	HOPR
<b>Descentralizado</b>	✓	✓	✓
<b>Enrutamiento multihop</b>	✓	✓	Opcional
<b>Relés incentivados</b>	✓	✗	✓
<b>Red escalable</b>	✓	✗	✓
<b>Protocolo de cifrado seguro y eficiente</b>	✓	✗	✓
<b>Gobernanza comunitaria de los nodos de retransmisión</b>	✓	✗	✗
<b>Resistencia robusta al análisis del tráfico</b>	✓	✓	✗
<b>Gran conjunto de anonimato</b>	✓	✗	✗
<b>Gran conjunto de anonimato</b>	✓	✗	✗

# NYM

Web  
[nymtech.net](http://nymtech.net)  
Github  
[@nymtech](https://github.com/nymtech)

Email  
[info@nymtech.net](mailto:info@nymtech.net)  
Twitter  
[@nymproject](https://twitter.com/nymproject)



Con Amor, Respeto y Admiración  
para la comunidad habla hispana de Nym  
Por DAOariwas.