

Mixnets

Ingenieria del
Caos contra la

Vigilancia Masiva

¿Quién es Red?

SecOpsDev

Formador, cuando me dejan

Activista tecnológico

- ✓ Soberanía tecnológica
- ✓ Defensor de la privacidad
- ✓ Cofundador de Hacklabs y M4H

Aprendiz de investigador



¿Quién es Red?

~~criptógrafo~~ ni ~~criptoanalista~~

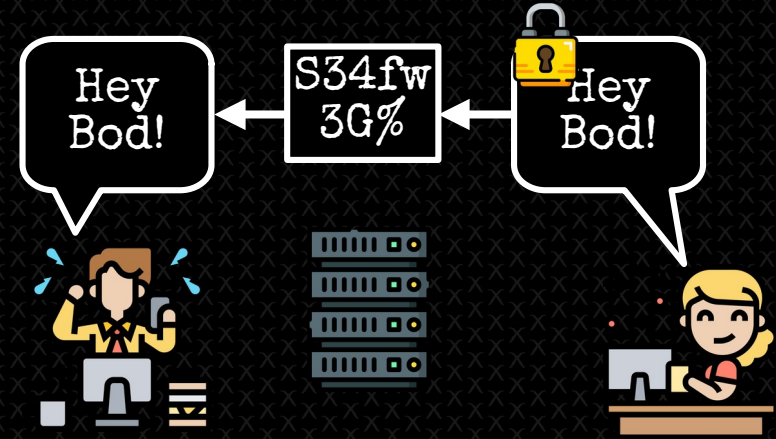


Soluciones de privacidad

VPN



E2EE



Tor

Chat control

La UE sigue queriendo inspeccionar tus fotos y mensajes privados



La propuesta "Chat Control" obligaría a la inspección de **todas** las comunicaciones digitales privadas, incluyendo mensajes cifrados y fotos. Esto amenaza los **derechos fundamentales de privacidad** y la seguridad digital de todos los ciudadanos de la Unión Europea.

8

ESTADOS MIEMBROS EN
CONTRA

12

ESTADOS MIEMBROS A
FAVOR

7

ESTADOS MIEMBROS
INDECISOS



Fight Chat Control



Metadatos / Tranceo



Direcciones IP

Revelan ubicación aproximada



Horarios y duración

Muestran rutinas y hábitos diarios



Frecuencia de conexión

Permite mapear relaciones sociales



Volumen de datos

Delata tipo de actividad (texto, llamada, vídeo)

Conspiranoico



Programa de la NSA PRISM / Upstream



2013

Vulnerabilidades de correlación en TOR

WIRED

Don't panic, Tor is still safe and here's why

2014



Paper metadatos

2017

WhatsApp security and role of metadata in preserving privacy

January 2017

DOI: [10.48550/arXiv.1701.06817](https://doi.org/10.48550/arXiv.1701.06817)

License · [CC BY-NC-SA 4.0](https://creativecommons.org/licenses/by-nc-sa/4.0/)

Authors:



Nidhi Rastogi
Rensselaer Polytechnic Institute



James Hendler

No todo es secreto

2023

The Washington Post

Not everything is secret in encrypted apps like iMessage and WhatsApp

Your cheat sheet to what information is encrypted and private in five chat apps, what is not and why the nuances matter.

Debate en Johns Hopkins



se puede conocer "todo" lo que
necesita para saber quién es cada
objetivo

Metadatos para
matar gente



Metadatos para matar gente



WIRED

Inside the NSA's Secret Tool for Mapping Your Social Network

Edward Snowden revealed the agency's phone-record tracking program. But thanks to "precomputed contact chaining," that database was much more powerful than anyone knew.

Conspiranoico?



Ingeniería de privacidad



Patrón de
comunicación

Mas allá del cifrado



Untraceable Electronic
Mail, Return Addresses,
and Digital Pseudonyms

David Chaum



- Uno de los CypherPunks mas destacados
- Su tesis doctoral es clave para entender la criptografía y las redes de criptomonedas
- Fundador de la Asociación Internacional de Investigación de Criptografía
- Chaumian Mixes (1981)
- Fundador de xx.network



Remailers



```
0100110011010 1
0100101100 10 1 1
010111
001100 0111010
101000111 1 00
1110 001 1 0
10010100 110 1 0 1
```

Mixmaster (1995)

Mixminion (2003)

cyphepunk

“la privacidad no es algo que se debiera pedir, sino algo que se debe tomar mediante la tecnología”

Las Mixnets - nodos

Simple Mixes
(Chaum mixes)

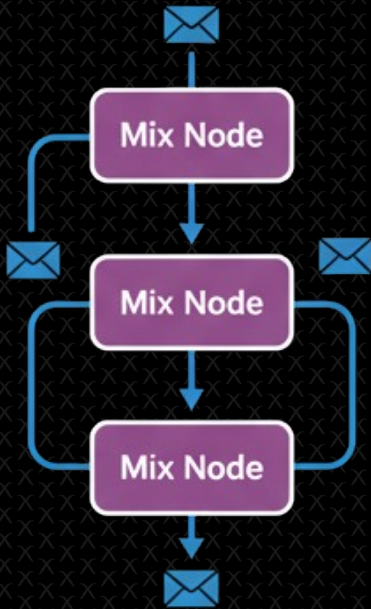


Mixes de parada
(stop and go mixes)

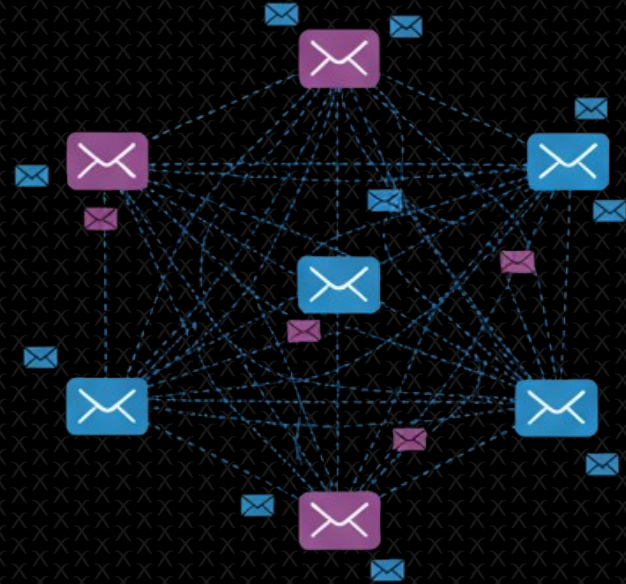


Topología en Mixnets

Mezcla en cascada
(cascade mixing)



Mezcla libre
(free route mixing)



TOR vs Mixnet

Tor



Uso interactivo
Onion Routing

Mixnets



Mensajería asíncrona
(email)
Seguridad contra análisis
tráfico
Acumula y mezcla

Soluciones actuales

Loopix

xx.network

Katzenpost

Nym

~~HOPE~~

~~ONION~~

Soluciones actuales

Loopix

2017

xx.network

Cmix

2016

Cmixx

2020

2021

Katzenpost

2019

~2025

Nym

2019

2023

Paper

Test

Producción

Avance tardío

Avances en
criptografía



Modelos
Mejorados



Incentivos



Demanda



Infraestructura



Paquetería Sphinx

Sphinx: A Compact and Provably
Secure Mix Format (2009)

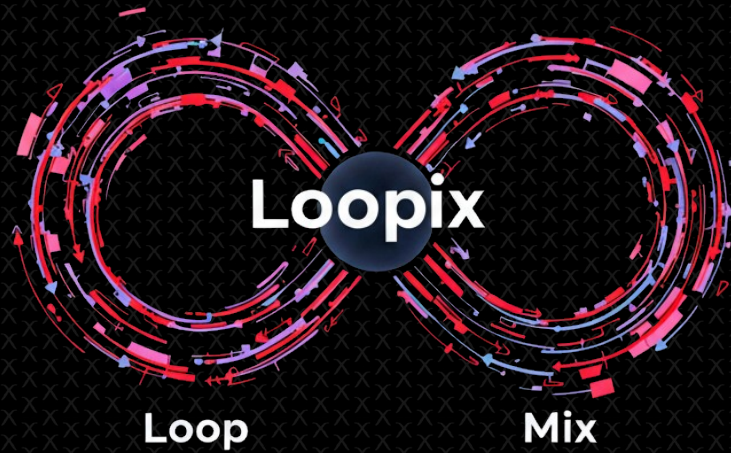


- Mismo tamaño de paquete
- Ocultación de ruta
- Claves efímeras

Base de la privacidad mixnets modernas



Loopix



The Loopix Anonymity System

Ania Piotrowska

Jamie Hayes

Tariq Elahi

Sebastian Meiser

George Danezis



NYM

Loopix - bases

Mezcla de Capas
(Layered Mixing)



Acumulan, baraja y
reenvían
Rompe correlación

Retrasos Exponenciales
(Poisson mixing)



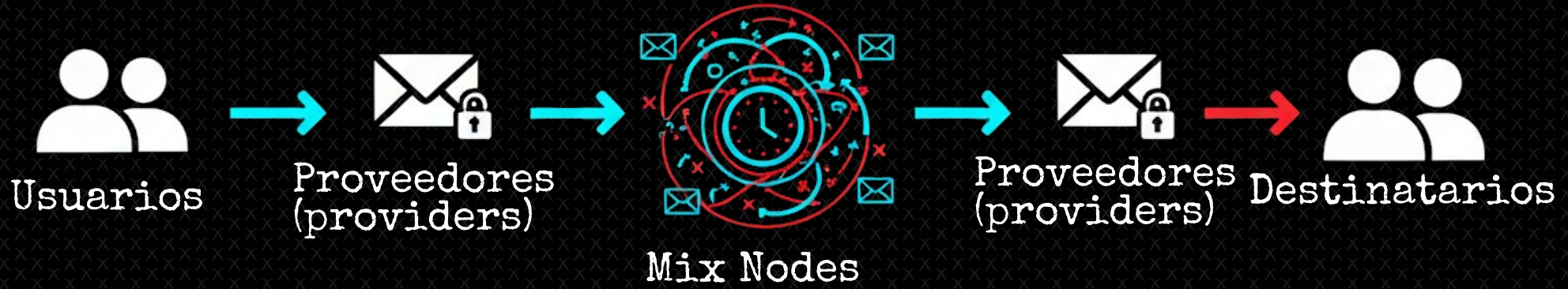
Tiempo aleatorio
Sin "memoria"
Dificultad análisis

Tráfico de Cobertura
(Cover Traffic)

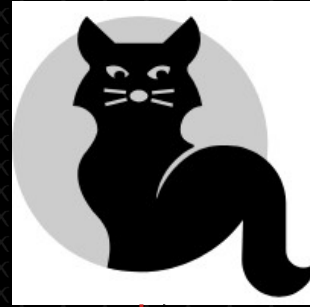


Mensajes falsos "loops"
Tráfico real
indistinguible

Loopix - nodos



Katzenpost - Post quantum



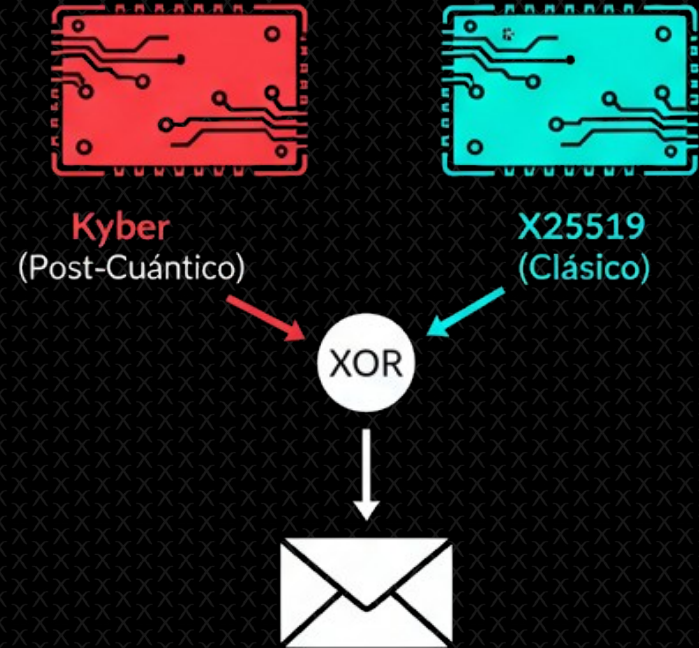
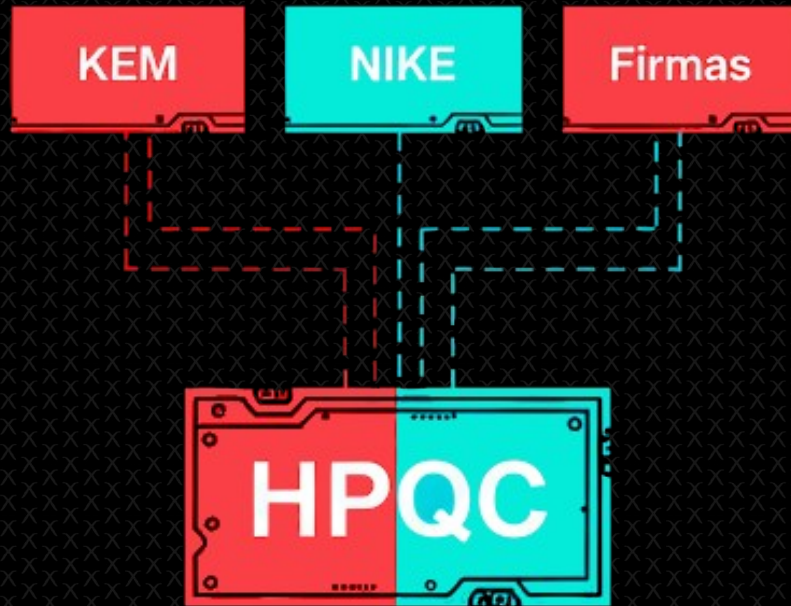
Herada de loopix

- Poisson mixing
- Cover Traffic
- Layered Mixing
- Empaquetado sphinx

Principal mejora

Criptografía
Post-Cuántica

Katzenpost - criptografía



Katzenpost - nodos

Usuario



Se conecta a la red
Envía mensajes

Authority Node



Oráculo de confianza
Listado de nodos
Documento consenso
Evita ataques sybil

Mix Node



Recibe, descifra, reenvía.
Tiempos aleatorios

Provider Node



Punto de contacto
Entrega mensajes

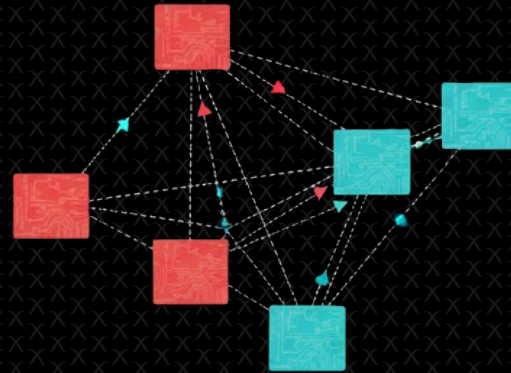
Katzenpost - Rutas

Modo cascada
(Ruta única)



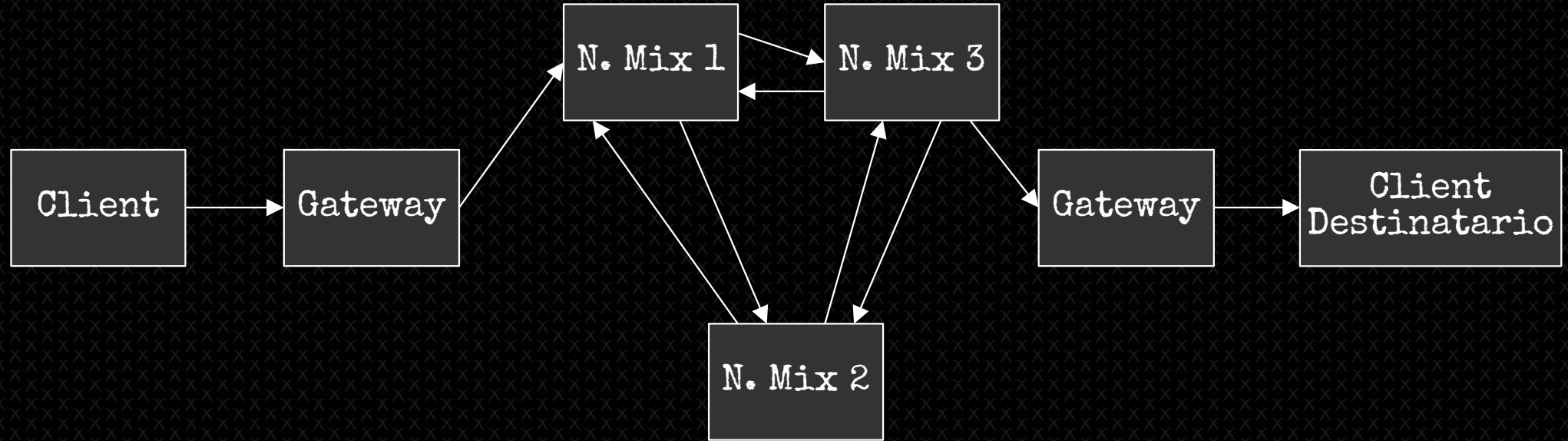
Ruta fija predefinida
Menos flexible

Modo Free-Route
(Rutas dinámicas)



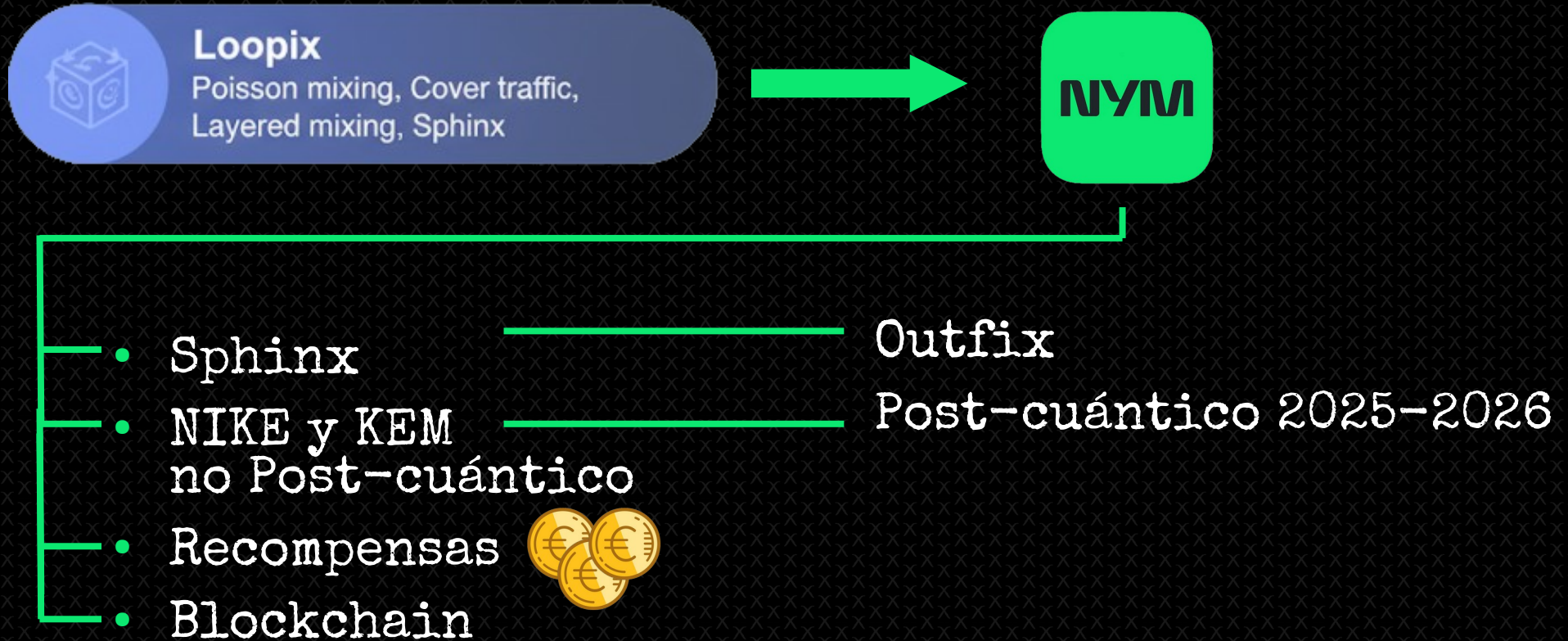
Ruta variable y aleatoria
Mayor flexibilidad y
resistencia

Katzenpost - flujo



3 Procesamiento en cada Mix Node:
Descripta capa
Añade retrasos (Poisson delays)
Mezcla mensajes de múltiples usuarios

N y m



Nym - Blockchain

Registro

Nodos, Stakes,
Reputación

Descentralizado

Sin registro

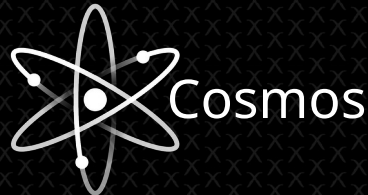


NYM Token
(ERC-20)

Reputación

Tiempo actividad

Rendimiento



Nym - Recompensas

PoW tipo PoM
basado de VRF

Selección aleatoria
Generación pruebas
criptográficas
Recompensar

Nym - nodes

Client (app NYM)



Punto de partida

Elige ruta (lgw 5mixes lgw)

Opc. PoW (antispam /
prioridad)

Opc. Pagos/recompensas

Gateway nodes



Entrada/salida de
red

Almacena mensajes
offline

Accesos VPN/API

Mix Nodes



Requieren staking
NYM tokens

Recompensas por PoM

Nym - nodes

Validators



Nym (cosmos)

Verifican PoM

Firman y publican
directorio

Recopilan métricas
(latencia, carga...)

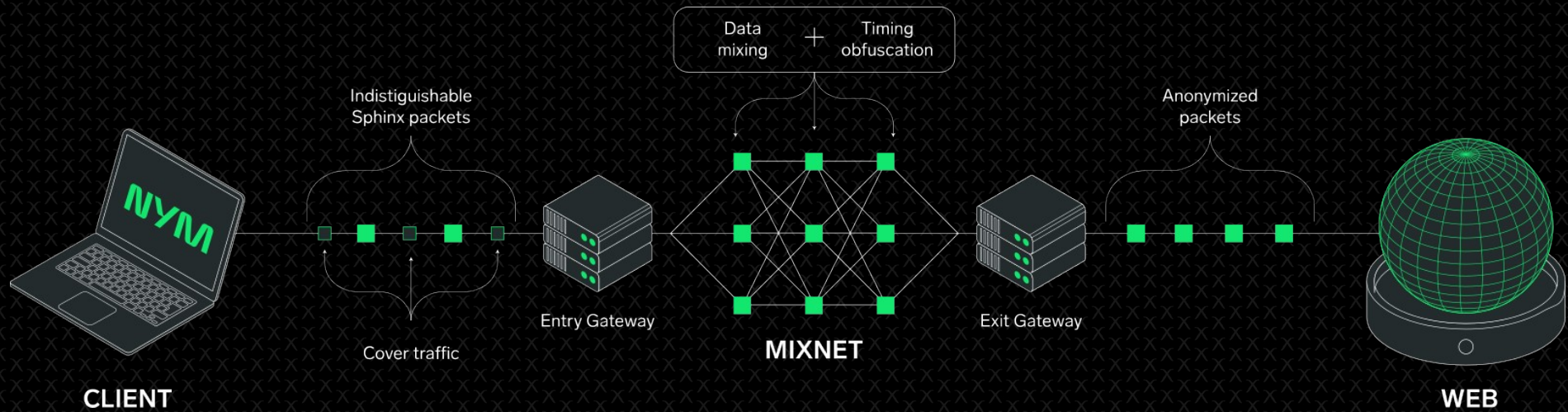
Observer/Monitor



Opcional

Verifican conectividad y
consultas al directorio

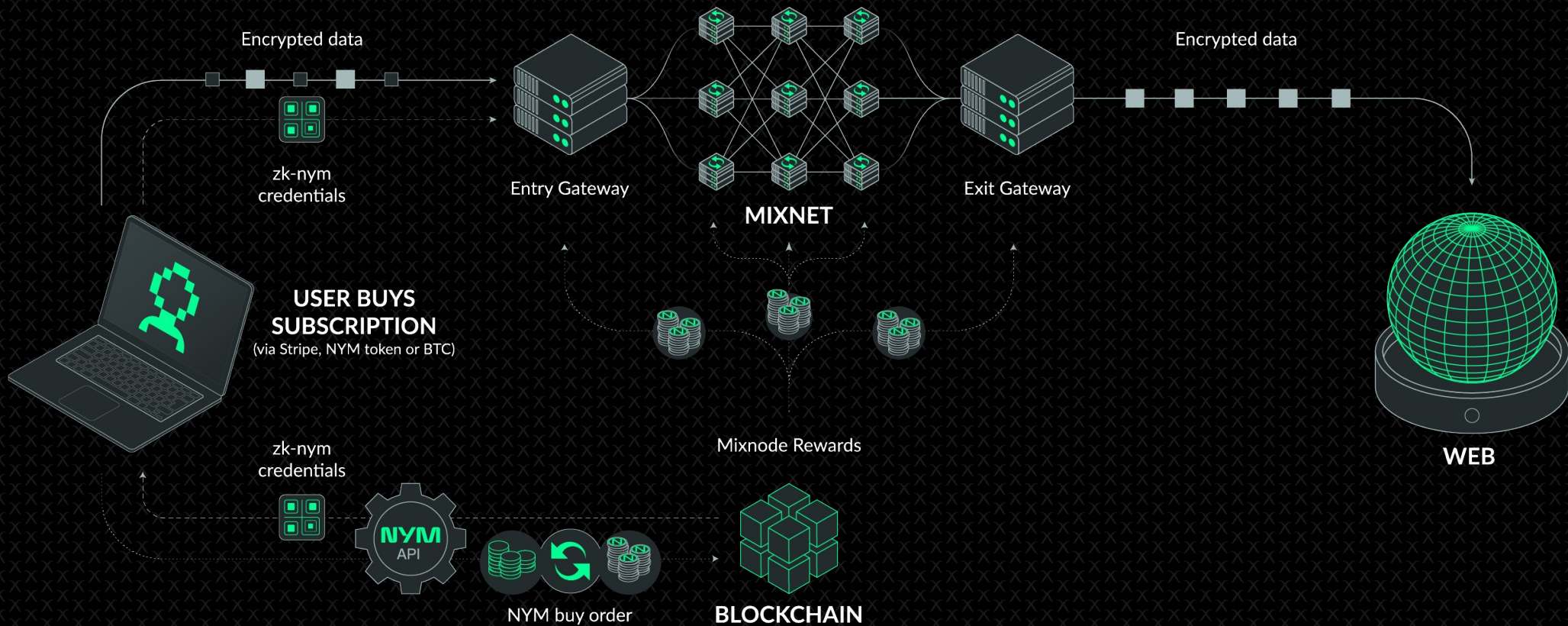
Nym - flujo



N y m



Nym - flujo



xx.network



Cmix (teoría) --> Cmixx (práctica)



Protocolo criptográfico

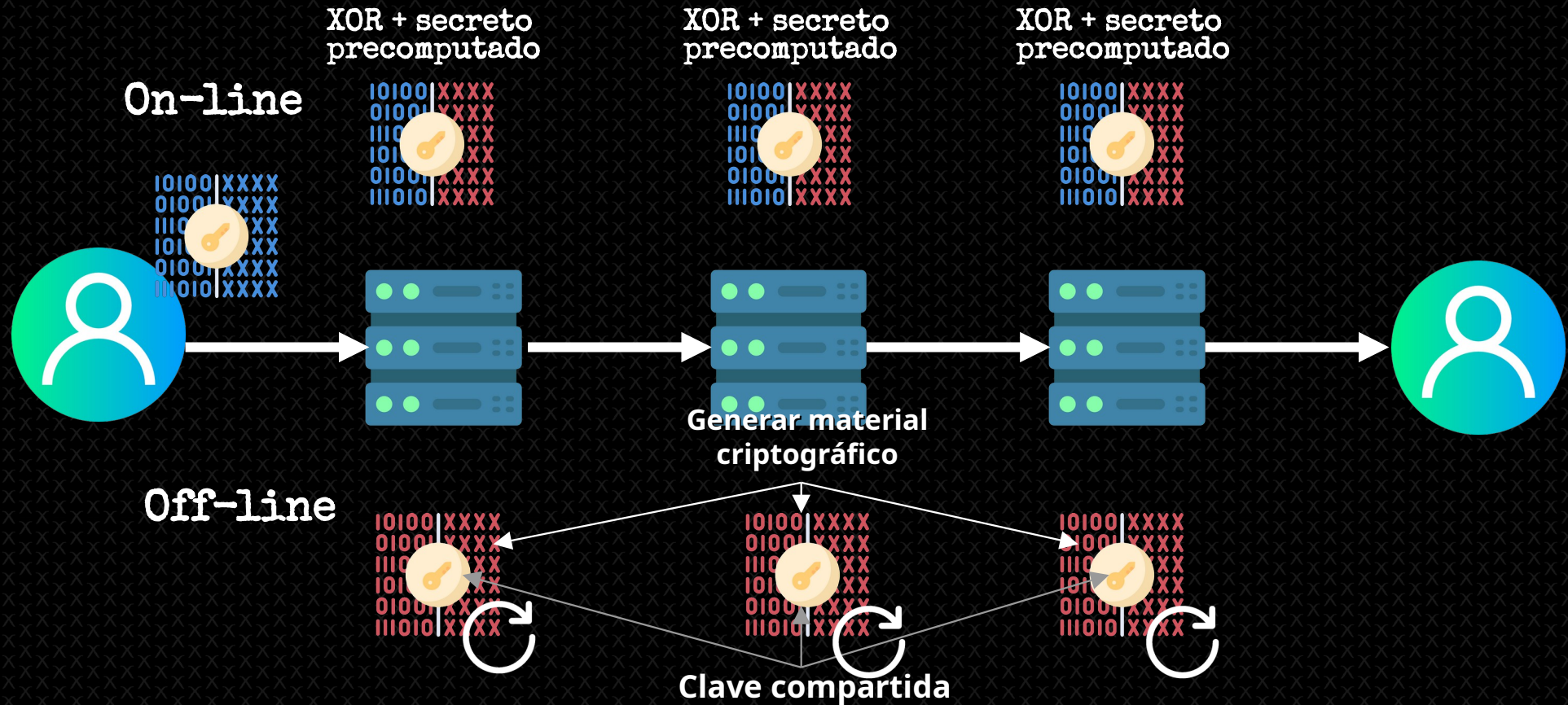
Precomputación

MultiParty Computation -
MPC

xx Network
(Ecosistema)



xx.network-funcionamiento



xx.network - nodos

Máquinas “físicas”

cMixxNode validator/mix node



Ejecuta el software cMixx y, además, actúa como validador de la cadena de bloques de xxnetwork

cMixx Gateway



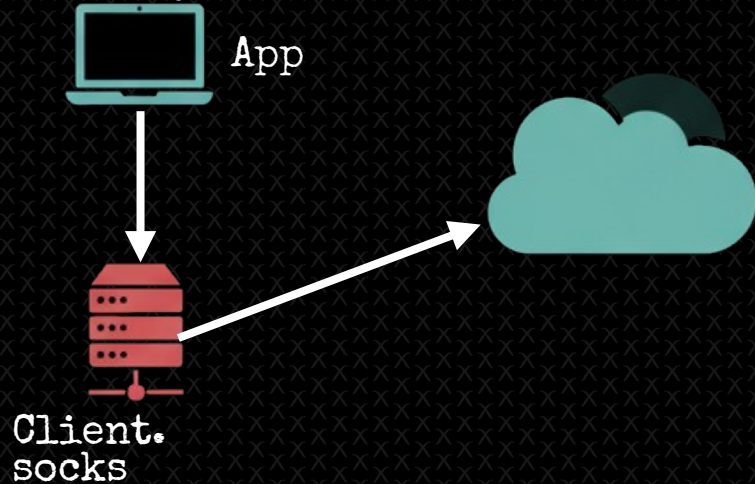
Ejecuta el mismo software cMixx pero funciona como nodo ligero (no como validador) y sirve de puerta de entrada/salida para el mixnet

Integraciones de Mixnet

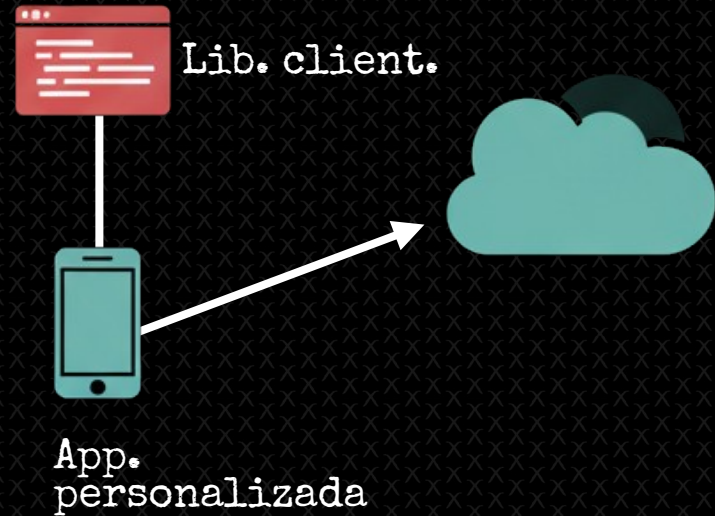
Usuarios finales

Desarrolladores

Proxy SOCKS



Integración Directa



Conclusiones

Hay grandes actores vigilando
las comunicaciones



Cmixx
(xx.network)

Si tu prioridad es la
velocidad y el
procesamiento masivo



Katzenpost

Si buscas una
plataforma de
investigación
abierta, sin token
y post-cuántica



Nym

Solución lista
para consumidores
con apps móviles

Gracias!! ¿Preguntas?



@feliz1984@mastodon.social



@ReD.1984



red@feliz1984.com