0DATA LAB · DOCUMENTO 008 · JULIO 2026

SPINA

La Columna Vertebral Criptográfica

Hadda TIKIJJA
0DATA Lab, Rennes, Francia

RESUMEN

Introducimos SPINA — un protocolo abierto y descentralizado de memoria inmunitaria para los organismos digitales. SPINA registra cada descubrimiento de amenaza, cada firma de comportamiento y cada anestesia exitosa en un registro blockchain inmutable, verificable criptográficamente por cualquier participante. A diferencia de las blockchains financieras, SPINA no utiliza ni prueba de trabajo ni token especulativo: su consenso por Prueba de Autoridad (PoA) evoluciona hacia una Prueba de Participación (PoS) donde el peso de un nodo refleja su contribución real a la red. La cadena es verificable en O(log n) mediante prueba Merkle. SPINA es un bien público digital bajo licencia MIT — El Lab creó el protocolo, la red pertenece a todos aquellos que la hacen funcionar. Es el cuarto pilar de Internet: después de TCP/IP (comunicación), HTTP (compartición) y DNS (nombrado), SPINA aporta la MEMORIA INMUNITARIA.

EN UNA FRASE

Este documento es la memoria. Describe el protocolo de blockchain con prueba de autoridad que registra cada firma de amenaza, cada anestesia exitosa, cada certificación — de manera inmutable, verificable, y descentralizada.

1. El Problema: La Amnesia de la Ciberseguridad

Cada día, miles de malwares son detectados, analizados y bloqueados en todo el mundo. Cada SOC, cada MSSP, cada empresa libra este combate de forma aislada. Un ransomware frustrado en París no inmuniza un hospital en Tokio. Una firma descubierta por un simbionte NOVA en Berlín no se comparte con un simbionte en São Paulo — o peor, se comparte a través de canales propietarios, lentos, centralizados, falibles.

Es la **amnesia de la ciberseguridad**. La industria gasta 200 mil millones de dólares al año para combatir amenazas que alguien, en algún lugar, ya ha vencido. El conocimiento existe — solo está prisionero en silos.

PRINCIPIO

Lo que recuerda sobrevive. Una amenaza vista una vez no debe poder dañar nunca más — en ningún lugar, para nadie, para siempre.

2. SPINA — Arquitectura

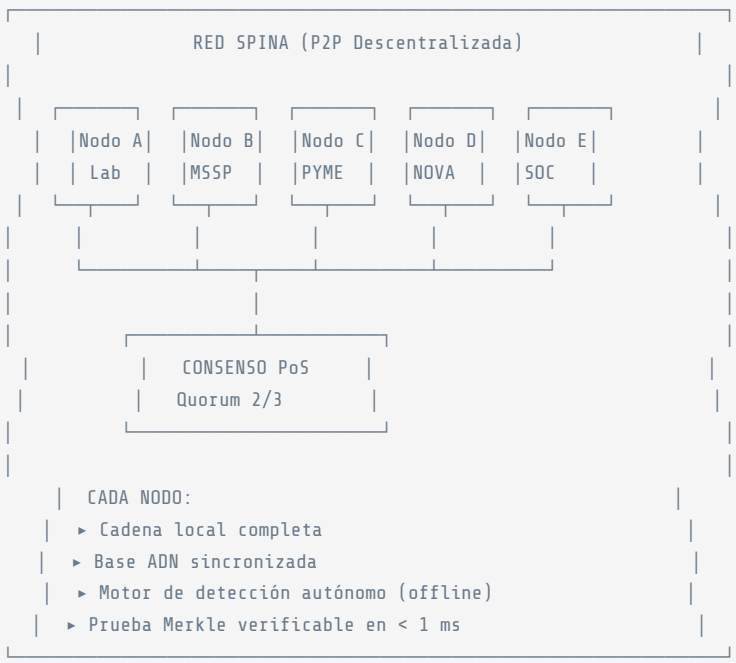

Figura 1: Arquitectura descentralizada de SPINA

2.1 El Bloque SPINA

DEFINICIÓN — BLOQUE SPINA

Un bloque SPINA B contiene:

▸ **prev_hash** — SHA-256 del bloque anterior

▸ **timestamp** — marca de tiempo UTC certificada

▸ **payload** — firma de amenaza, hash de comportamiento, o informe de anestesia

▸ **merkle_root** — raíz del árbol Merkle de las firmas activas

▸ **validator_sig** — firma Ed25519 del nodo validador

La validez de B es verificable por cualquier nodo en una operación de hashing.

2.2 Árbol Merkle — Verificación en O(log n)

La base ADN completa (25K+ firmas) está estructurada en árbol de Merkle. Para verificar que una firma específica pertenece a la base, un nodo no necesita descargar las 25K entradas — recibe una prueba Merkle de $\log_2(25000) \approx 15$ hashes, es decir, aproximadamente 480 bytes. El tiempo de verificación es inferior a 1 milisegundo.

2.3 Consenso Evolutivo

FASE	NODOS	CONSENSO	ROL LAB
Bootstrap	< 100	PoA (validadoras conocidas)	Operador principal
Crecimiento	100–1000	PoS híbrido	Un validador entre otros
Madurez	1000+	PoS completo	Nodo como los demás

3. SPINA como Bien Público

3.1 Licencia MIT — Cero Barreras

SPINA se publica bajo licencia MIT. Cualquiera puede usarlo, modificarlo, redistribuirlo, integrarlo en sus productos. Sin royalties. Sin contrato. Sin permiso. Es una infraestructura pública — como TCP/IP, como HTTP, como las vacunas.

MODELO ECONÓMICO

SPINA = gratuito. El protocolo es un bien común. Como el agua potable. Como el conocimiento.

NOVA = de pago. El organismo que utiliza SPINA — cockpit molecular, Kenza, injerto, anestesia — es el producto NOVA.

Es el modelo Linux + Red Hat. HTTP + Google. El protocolo es libre. El valor está en la implementación.

3.2 Por Qué Descentralizado

Una memoria centralizada es falible. El data center puede caer. La empresa puede desaparecer. El Estado puede censurar. SPINA no tiene centro — por tanto, no tiene blanco, no tiene punto único de fallo, no tiene autoridad que pueda alterar la verdad.

El Lab creó el protocolo. Pero el día en que el Lab ya no exista, SPINA continúa. Porque la memoria inmunitaria de la humanidad digital no debe depender de una sola entidad.

4. Implementación Técnica

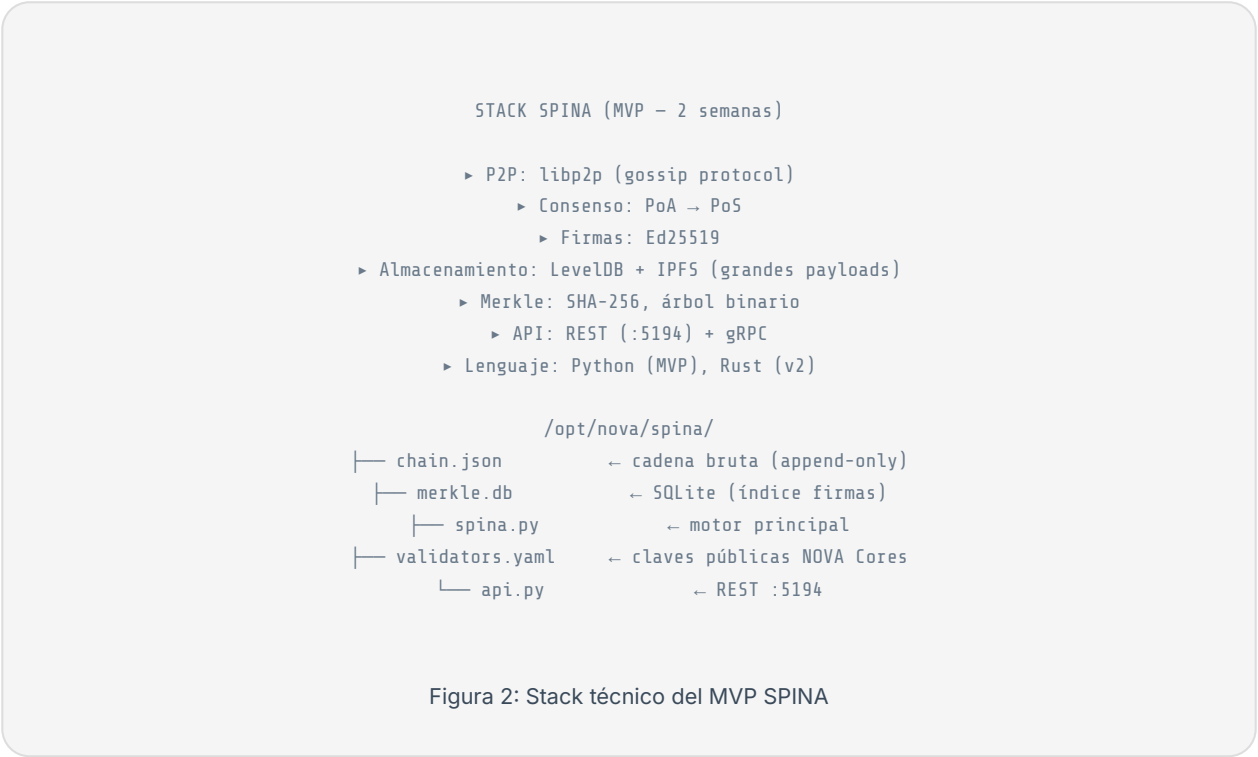

Figura 2: Stack técnico del MVP SPINA

Un nodo SPINA completo ocupa menos de 50 MB de almacenamiento, utiliza menos del 1% de CPU en régimen permanente, y consume aproximadamente 10 MB/día de ancho de banda. Funciona en un Raspberry Pi, un viejo servidor, o en contenedor Docker.

5. Integración con el Ecosistema NOVA

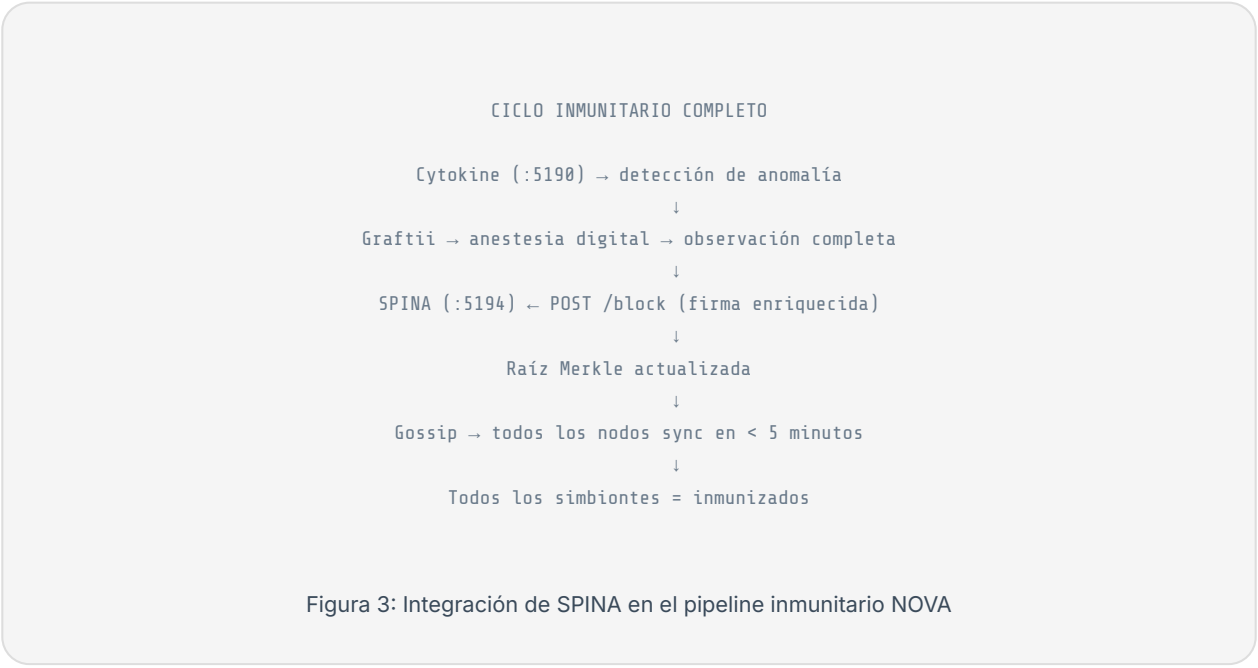

Figura 3: Integración de SPINA en el pipeline inmunitario NOVA

6. Extensiones Naturales

Convergencia Estratégica. Con SPINA, el espacio de las estrategias maliciosas se reduce con cada registro. Tras 10 000 malwares anestesiados, el sistema reconoce un ransomware en el primer paquete — antes incluso de que haya comenzado su primera acción significativa. Véase Documento 000 para el teorema completo.

Identidad de los Simbiontes. Cada NOVA Core, cada µNOVA posee una identidad on-chain verificable. Anti-spoofing criptográfico: ningún simbionte puede usurpar la identidad de otro.

Auditoría y Conformidad. NIS2, ISO 27001, ExpertCyber — cada acción de seguridad está fechada y firmada en SPINA. El auditor verifica la integridad mediante prueba Merkle. Cero falsificación posible.

7. Conclusión

SPINA es la respuesta al problema de la amnesia. La ciberseguridad tradicional combate las mismas amenazas miles de veces, en paralelo, sin compartir jamás sus victorias. SPINA transforma cada victoria en inmunidad colectiva.

No es un producto. Es la memoria del mundo digital — abierta, descentralizada, inmutable.

SPINA

Una amenaza vista una vez. Nunca más en ningún lugar. Para nadie. Para siempre.

Lo que recuerda sobrevive.

Referencias

[1] S. Nakamoto, « Bitcoin: A Peer-to-Peer Electronic Cash System », 2008.

[2] D. Deutsch, C. Marletto, « Constructor theory of information », Proc. Royal Society A, 2015. arXiv:1405.5563.

[3] R.C. Merkle, « A Digital Signature Based on a Conventional Encryption Function », CRYPTO '87, 1987.

[4] J. Benet, « IPFS — Content Addressed, Versioned, P2P File System », arXiv:1407.3561, 2014.

[5] H. TIKIJJA, « La Ley — Fundamento Unificado de los Organismos Digitales », 0DATA Lab, Documento 000, 2026.

[6] H. TIKIJJA, « El Sistema Inmunitario de las Infraestructuras », 0DATA Lab, Documento 005, 2026.

[7] C. Kolias et al., « Swarm Immunity in Cybersecurity », IEEE COMST, 2024.

[8] J. Warnat-Herresthal et al., « Swarm Learning », Nature, 594, 265–270, 2021.