0DATA LAB · PAPER 008 · JULY 2026

SPINA

The Cryptographic Spine

Hadda TIKIJJA
0DATA Lab, Rennes, France

ABSTRACT

We introduce SPINA — an open and decentralized immune memory protocol for digital organisms. SPINA records every threat discovery, every behavioral signature, and every successful anesthesia in an immutable blockchain ledger, cryptographically verifiable by any participant. Unlike financial blockchains, SPINA uses neither proof-of-work nor speculative tokens: its consensus evolves from Proof-of-Authority (PoA) toward Proof-of-Stake (PoS) where a node's weight reflects its actual contribution to the network. The chain is verifiable in O(log n) via Merkle proof. SPINA is a digital public good under the MIT license — The Lab created the protocol, the network belongs to everyone who runs it. It is the fourth pillar of the Internet: after TCP/IP (communication), HTTP (sharing), and DNS (naming), SPINA brings IMMUNE MEMORY.

IN ONE SENTENCE

This paper is the memory. It describes the proof-of-authority blockchain protocol that records every threat signature, every successful anesthesia, every certification — immutably, verifiably, and decentralized.

1. The Problem: Cybersecurity Amnesia

Every day, thousands of malware strains are detected, analyzed, and blocked across the world. Every SOC, every MSSP, every company fights this battle in isolation. A ransomware thwarted in Paris does not immunize a hospital in Tokyo. A signature discovered by a NOVA symbiont in Berlin is not shared with a symbiont in São Paulo — or worse, it is shared through proprietary, slow, centralized, fallible channels.

This is **cybersecurity amnesia**. The industry spends 200 billion dollars per year fighting threats that someone, somewhere, has already defeated. The knowledge exists — it is merely trapped in silos.

PRINCIPLE

That which remembers, survives. A threat seen once must never be able to harm again — nowhere, for no one, forever.

2. SPINA — Architecture

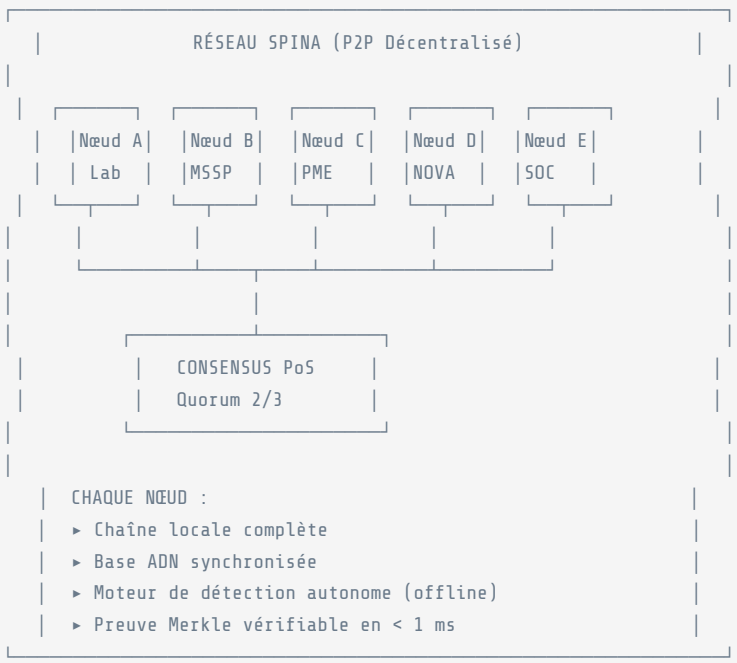

Figure 1: Decentralized Architecture of SPINA

2.1 The SPINA Block

DEFINITION – SPINA BLOCK

A SPINA block B contains:

▸ prev_hash — SHA-256 of the previous block

▸ timestamp — certified UTC timestamp

▸ payload — threat signature, behavioral hash, or anesthesia report

▸ merkle_root — root of the Merkle tree of active signatures

▸ validator_sig — Ed25519 signature of the validating node

The validity of B is verifiable by any node in a single hash operation.

2.2 Merkle Tree — O(log n) Verification

The complete DNA base (25K+ signatures) is structured as a Merkle tree. To verify that a specific signature belongs to the base, a node does not need to download all 25K entries — it receives a Merkle proof of $\log_2(25000) \approx 15$ hashes, approximately 480 bytes. Verification time is under 1 millisecond.

2.3 Evolving Consensus

PHASE	NODES	CONSENSUS	LAB ROLE
Bootstrap	< 100	PoA (known validators)	Primary operator
Growth	100–1000	Hybrid PoS	One validator among others
Maturity	1000+	Full PoS	A node like any other

3. SPINA as a Public Good

3.1 MIT License — Zero Barriers

SPINA is published under the MIT license. Anyone can use it, modify it, redistribute it, integrate it into their products. No royalties. No contracts. No permission. It is public infrastructure — like TCP/IP, like HTTP, like vaccines.

ECONOMIC MODEL

SPINA = free. The protocol is a common good. Like drinking water. Like knowledge.

NOVA = paid. The organism that uses SPINA — molecular cockpit, Kenza, graft, anesthesia — is the NOVA product.

This is the Linux + Red Hat model. HTTP + Google. The protocol is free. The value is in the implementation.

3.2 Why Decentralized

A centralized memory is fallible. The data center can go down. The company can disappear. The State can censor. SPINA has no center — therefore no target, no single point of failure, no authority that can alter the truth.

The Lab created the protocol. But the day the Lab no longer exists, SPINA continues. Because the immune memory of digital humanity must not depend on a single entity.

4. Technical Implementation

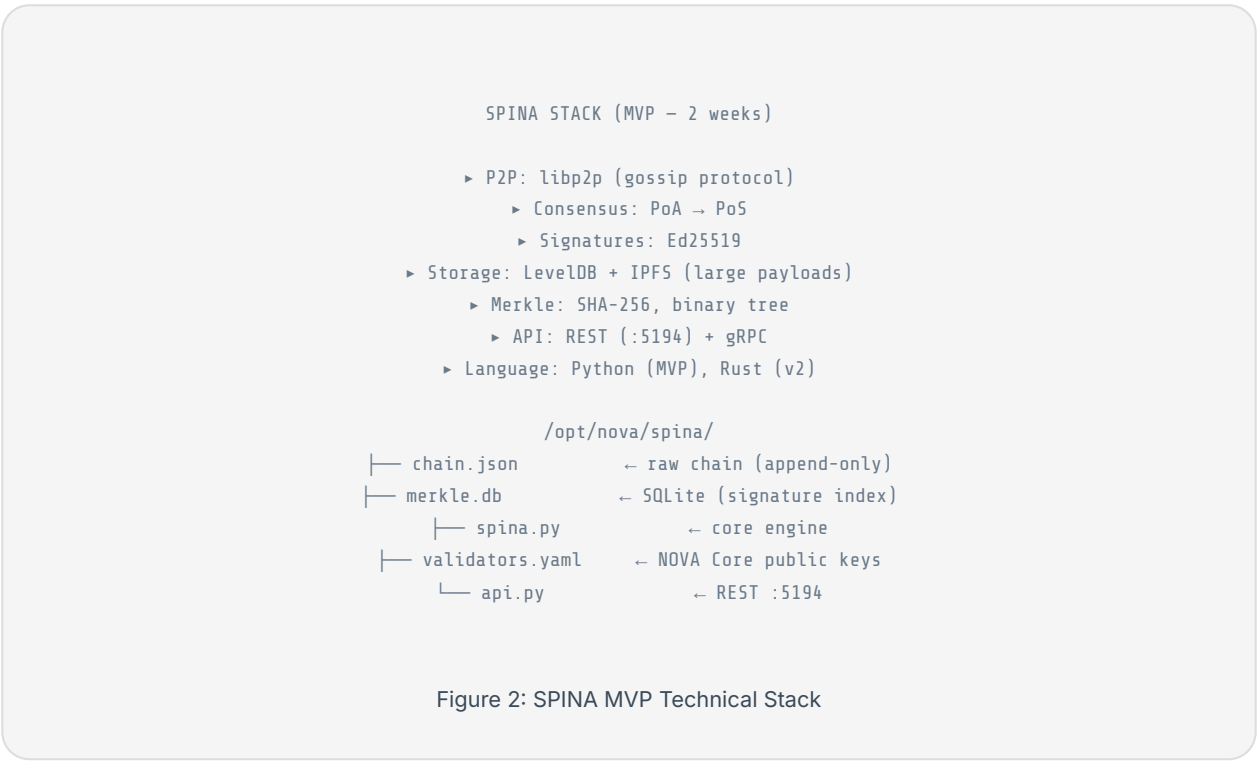

Figure 2: SPINA MVP Technical Stack

A full SPINA node occupies less than 50 MB of storage, uses less than 1% CPU in steady state, and consumes approximately 10 MB/day of bandwidth. It runs on a Raspberry Pi, an old server, or in a Docker container.

5. Integration with the NOVA Ecosystem

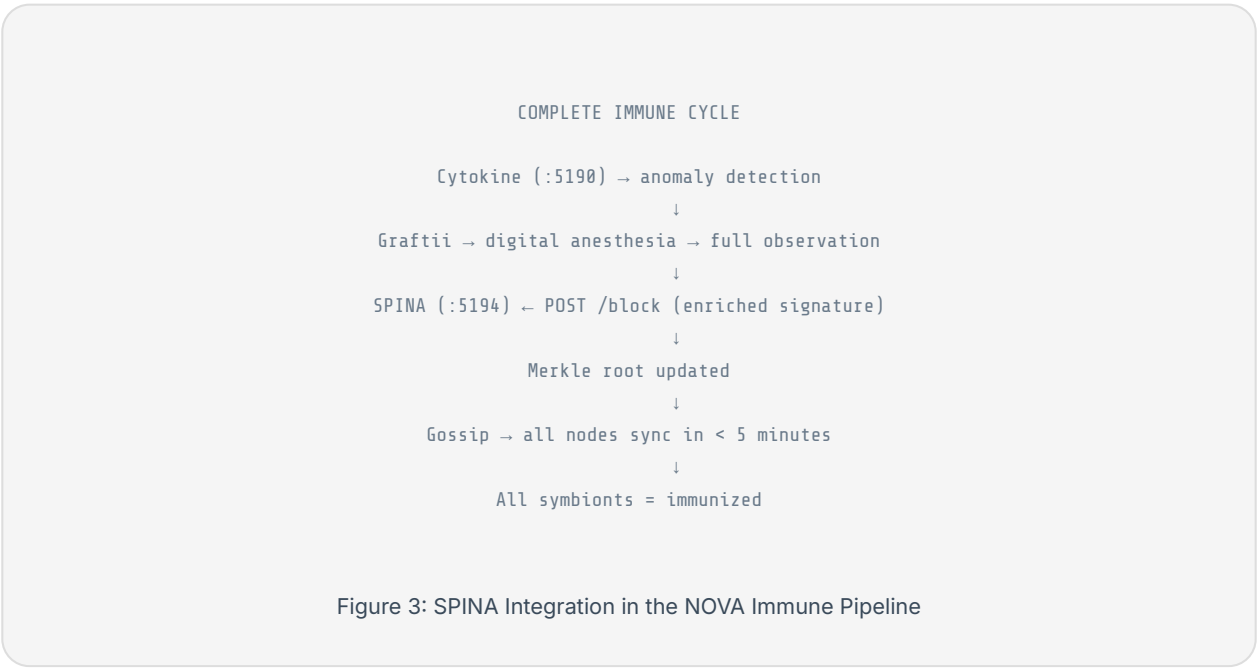

Figure 3: SPINA Integration in the NOVA Immune Pipeline

6. Natural Extensions

Strategic Convergence. With SPINA, the space of malicious strategies shrinks with every record. After 10,000 anesthetized malware strains, the system recognizes a ransomware on the first packet — before it has even begun its first significant action. See Paper 000 for the full theorem.

Symbiont Identity. Every NOVA Core, every µNOVA possesses a verifiable on-chain identity. Cryptographic anti-spoofing: no symbiont can impersonate another.

Audit and Compliance. NIS2, ISO 27001, ExpertCyber — every security action is timestamped and signed in SPINA. The auditor verifies integrity via Merkle proof. Zero falsification possible.

7. Conclusion

SPINA is the answer to the amnesia problem. Traditional cybersecurity fights the same threats thousands of times, in parallel, without ever sharing its victories. SPINA transforms every victory into collective immunity.

This is not a product. It is the memory of the digital world — open, decentralized, immutable.

SPINA

A threat seen once. Never again anywhere. For no one. Forever.

That which remembers, survives.

References

[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, "The Law — Unified Foundation of Digital Organisms", 0DATA Lab, Paper 000, 2026.

[6] H. TIKIJJA, "The Immune System of Infrastructures", 0DATA Lab, Paper 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.