SPINA

La Colonne Vertébrale Cryptographique

Hadda TIKIJJA
0DATA Lab, Rennes, France

RÉSUMÉ

Nous introduisons **SPINA** — un protocole ouvert et décentralisé de mémoire immunitaire pour les organismes numériques. SPINA enregistre chaque découverte de menace, chaque signature de comportement et chaque anesthésie réussie dans un registre blockchain immuable, vérifiable cryptographiquement par tout participant. Contrairement aux blockchains financières, SPINA n'utilise ni preuve de travail ni token spéculatif : son consensus par Preuve d'Autorité (PoA) évolue vers une Preuve d'Enjeu (PoS) où le poids d'un nœud reflète sa contribution réelle au réseau. La chaîne est vérifiable en O(log n) via preuve Merkle. SPINA est un bien public numérique sous licence MIT — Le Lab a créé le protocole, le réseau appartient à tous ceux qui le font tourner. C'est le quatrième pilier de l'Internet : après TCP/IP (communication), HTTP (partage) et DNS (nommage), SPINA apporte la MÉMOIRE IMMUNITAIRE.

EN UNE PHRASE

Ce papier est la mémoire. Il décrit le protocole de blockchain à preuve d'autorité qui enregistre chaque signature de menace, chaque anesthésie réussie, chaque certification — de manière immuable, vérifiable, et décentralisée.

1. Le Problème : L'Amnésie de la Cybersécurité

Chaque jour, des milliers de malwares sont détectés, analysés et bloqués à travers le monde. Chaque SOC, chaque MSSP, chaque entreprise mène ce combat isolément. Un ransomware déjoué à Paris n'immunise pas un hôpital à Tokyo. Une signature découverte par un symbiote NOVA à Berlin n'est pas partagée avec un symbiote à São Paulo — ou pire, elle est partagée via des canaux propriétaires, lents, centralisés, faillibles.

C'est **l'amnésie de la cybersécurité**. L'industrie dépense 200 milliards de dollars par an pour combattre des menaces que quelqu'un, quelque part, a déjà vaincues. La connaissance existe — elle est juste prisonnière de silos.

PRINCIPE

Ce qui se souvient survit. Une menace vue une fois ne doit plus jamais pouvoir nuire — nulle part, pour personne, pour toujours.

2. SPINA — Architecture

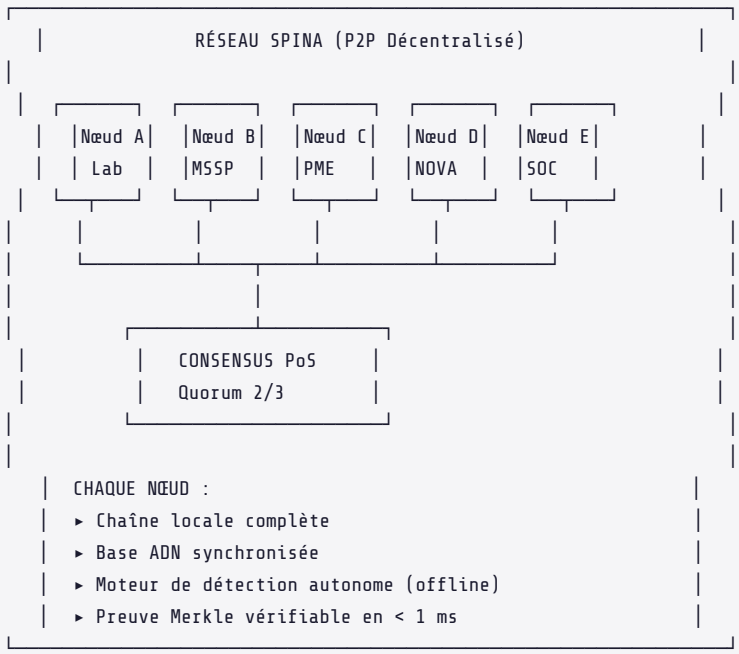

Figure 1 : Architecture décentralisée de SPINA

2.1 Le Bloc SPINA

DÉFINITION – BLOC SPINA

Un bloc SPINA B contient :

▸ **prev_hash** — SHA-256 du bloc précédent

▸ **timestamp** — horodatage UTC certifié

▸ **payload** — signature de menace, hash de comportement, ou compte-rendu d'anesthésie

▸ **merkle_root** — racine de l'arbre Merkle des signatures actives

▸ **validator_sig** — signature Ed25519 du nœud validateur

La validité de B est vérifiable par tout nœud en une opération de hachage.

2.2 Arbre Merkle — Vérification en O(log n)

La base ADN complète (25K+ signatures) est structurée en arbre de Merkle. Pour vérifier qu'une signature spécifique appartient à la base, un nœud n'a pas besoin de télécharger les 25K entrées — il reçoit une preuve Merkle de $\log_2(25000) \approx 15$ hachages, soit environ 480 octets. Le temps de vérification est inférieur à 1 milliseconde.

2.3 Consensus Évolutif

PHASE	NŒUDS	CONSENSUS	RÔLE LAB
Bootstrap	< 100	PoA (validatrices connues)	Opérateur principal
Croissance	100–1000	PoS hybride	Un validateur parmi d'autres
Maturité	1000+	PoS complet	Nœud comme les autres

3. SPINA comme Bien Public

3.1 Licence MIT — Zéro Barrière

SPINA est publié sous licence MIT. N'importe qui peut l'utiliser, le modifier, le redistribuer, l'intégrer à ses produits. Pas de royalties. Pas de contrat. Pas de permission. C'est une infrastructure publique — comme TCP/IP, comme HTTP, comme les vaccins.

MODÈLE ÉCONOMIQUE

SPINA = gratuit. Le protocole est un bien commun. Comme l'eau potable. Comme la connaissance.

NOVA = payant. L'organisme qui utilise SPINA — cockpit moléculaire, Kenza, greffe, anesthésie — est le produit NOVA.

C'est le modèle Linux + Red Hat. HTTP + Google. Le protocole est libre. La valeur est dans l'implémentation.

3.2 Pourquoi Décentralisé

Une mémoire centralisée est faillible. Le data center peut tomber. L'entreprise peut disparaître. L'État peut censurer. SPINA n'a pas de centre — donc pas de cible, pas de point unique de défaillance, pas d'autorité qui peut altérer la vérité.

Le Lab a créé le protocole. Mais le jour où le Lab n'existe plus, SPINA continue. Parce que la mémoire immunitaire de l'humanité numérique ne doit pas dépendre d'une seule entité.

4. Implémentation Technique

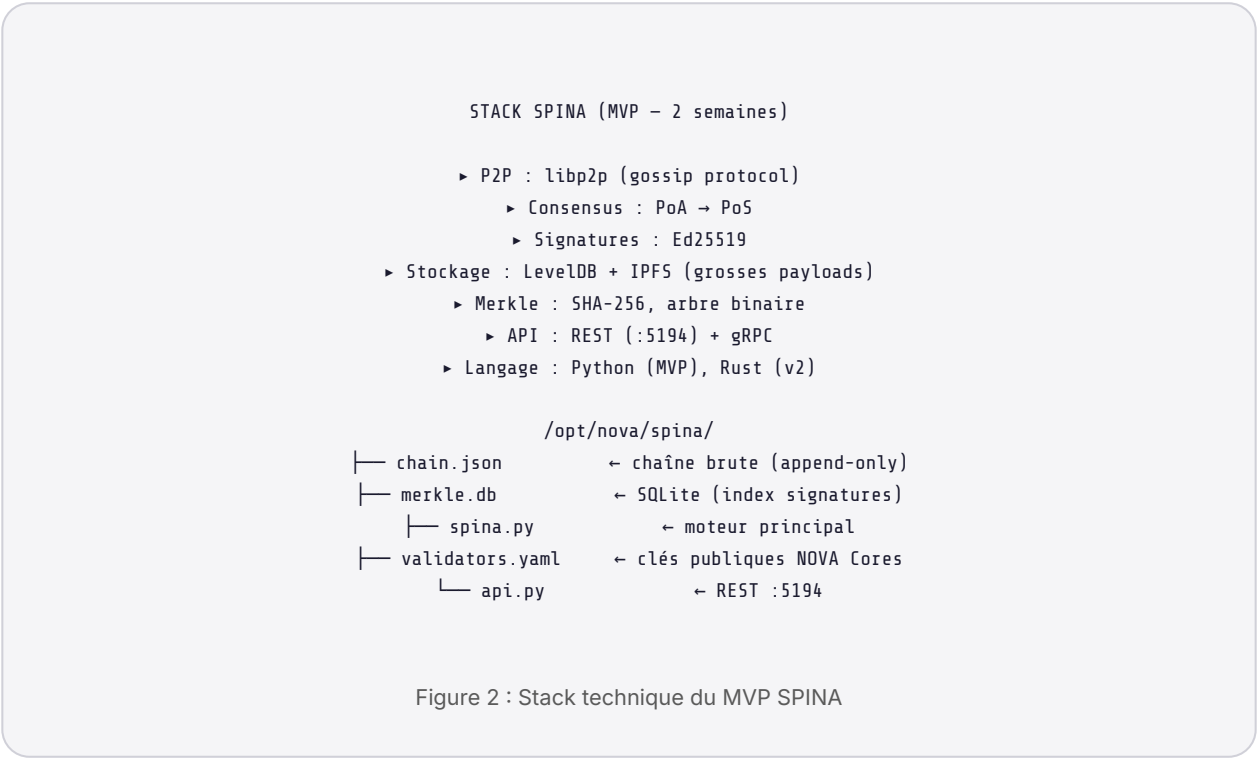

Figure 2 : Stack technique du MVP SPINA

Un nœud SPINA complet occupe moins de 50 Mo de stockage, utilise moins de 1% de CPU en régime permanent, et consomme environ 10 Mo/jour de bande passante. Il tourne sur un Raspberry Pi, un vieux serveur, ou en conteneur Docker.

5. Intégration avec l'Écosystème NOVA

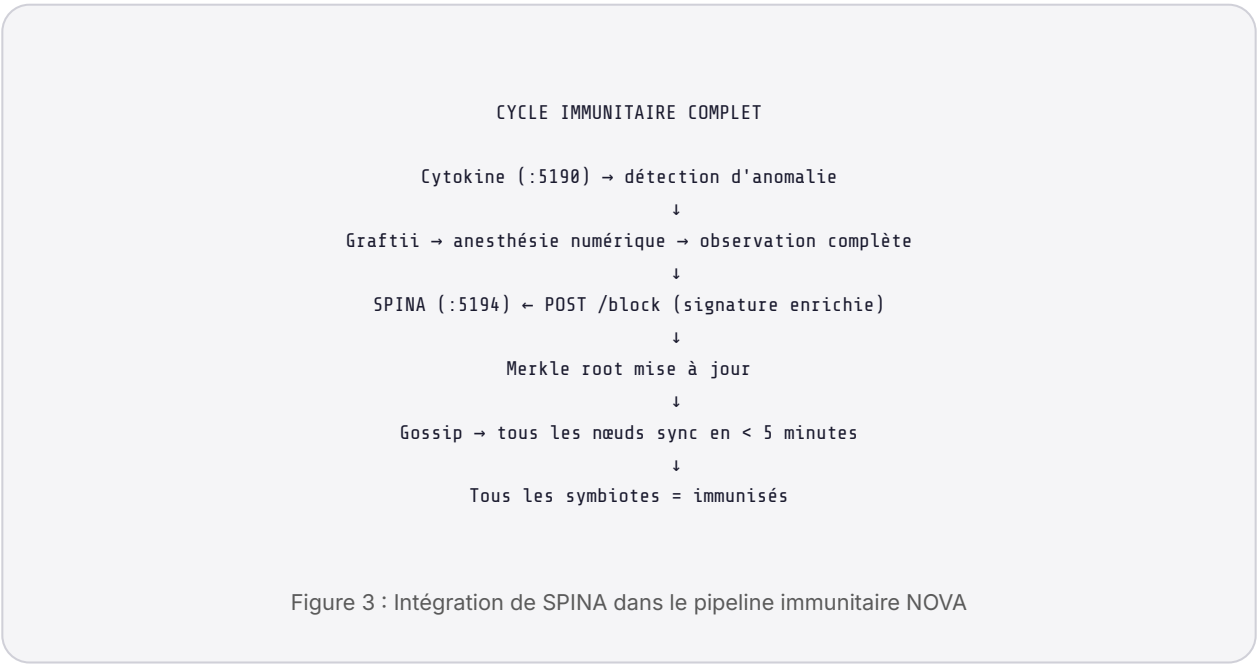

Figure 3 : Intégration de SPINA dans le pipeline immunitaire NOVA

6. Extensions Naturelles

Convergence Stratégique. Avec SPINA, l'espace des stratégies malveillantes se réduit à chaque enregistrement. Après 10 000 malwares anesthésiés, le système reconnaît un ransomware au premier paquet — avant même qu'il n'ait commencé sa première action significative. Voir Papier 000 pour le théorème complet.

Identité des Symbiotes. Chaque NOVA Core, chaque µNOVA possède une identité on-chain vérifiable. Anti-spoofing cryptographique : aucun symbiote ne peut usurper l'identité d'un autre.

Audit et Conformité. NIS2, ISO 27001, ExpertCyber — chaque action de sécurité est horodatée et signée dans SPINA. L'auditeur vérifie l'intégrité par preuve Merkle. Zéro falsification possible.

7. Conclusion

SPINA est la réponse au problème de l'amnésie. La cybersécurité traditionnelle combat les mêmes menaces des milliers de fois, en parallèle, sans jamais partager ses victoires. SPINA transforme chaque victoire en immunité collective.

Ce n'est pas un produit. C'est la mémoire du monde numérique — ouverte, décentralisée, immuable.

SPINA

Une menace vue une fois. Plus jamais nulle part. Pour personne. Pour toujours.

Ce qui se souvient survit.

Références

[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 Loi — Fondement Unifié des Organismes Numériques », 0DATA Lab, Papier 000, 2026.

[6] H. TIKIJJA, « Le Système Immunitaire des Infrastructures », 0DATA Lab, Papier 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.