SPINA

العمود الفقري التشفيري

Hadda TIKIJJA
0DATA Lab, Rennes, France

ملخص

نقدم SPINA — بروتوكولاً مفتوحاً ولامركزياً للذاكرة المناعية للكائنات الرقمية. يسجل SPINA كل اكتشاف تهديد، وكل توقيع سلوكي، وكل تخدير ناجح في سجل blockchain غير قابل للتغيير، قابل للتحقق تشفيرياً من قبل أي مشارك. وخلافاً لسلاسل الكتل المالية، لا يستخدم SPINA إثبات العمل ولا الرموز المضاربية: بل إن إجماعه عبر إثبات السلطة (PoA) يتطور نحو إثبات الحصة (PoS) حيث يعكس وزن العقدة مساهمتها الفعلية في الشبكة. السلسلة قابلة للتحقق بتعقيد O(log n) عبر برهان Merkle. SPINA هو صالح عام رقمي بموجب رخصة MIT — أنشأ المختبر البروتوكول، والشبكة ملك لكل من يشغّلها. إنه الركيزة الرابعة للإنترنت: بعد TCP/IP (الاتصال)، وHTTP (المشاركة)، وDNS (التسمية)، يقدم SPINA الذاكرة المناعية.

في جملة واحدة

هذه الورقة هي الذاكرة. تصف بروتوكول blockchain بإثبات السلطة الذي يسجل كل توقيع تهديد، وكل تخدير ناجح، وكل شهادة — بشكل غير قابل للتغيير، وقابل للتحقق، ولامركزي.

١. المشكلة: فقدان الذاكرة في الأمن السيبراني

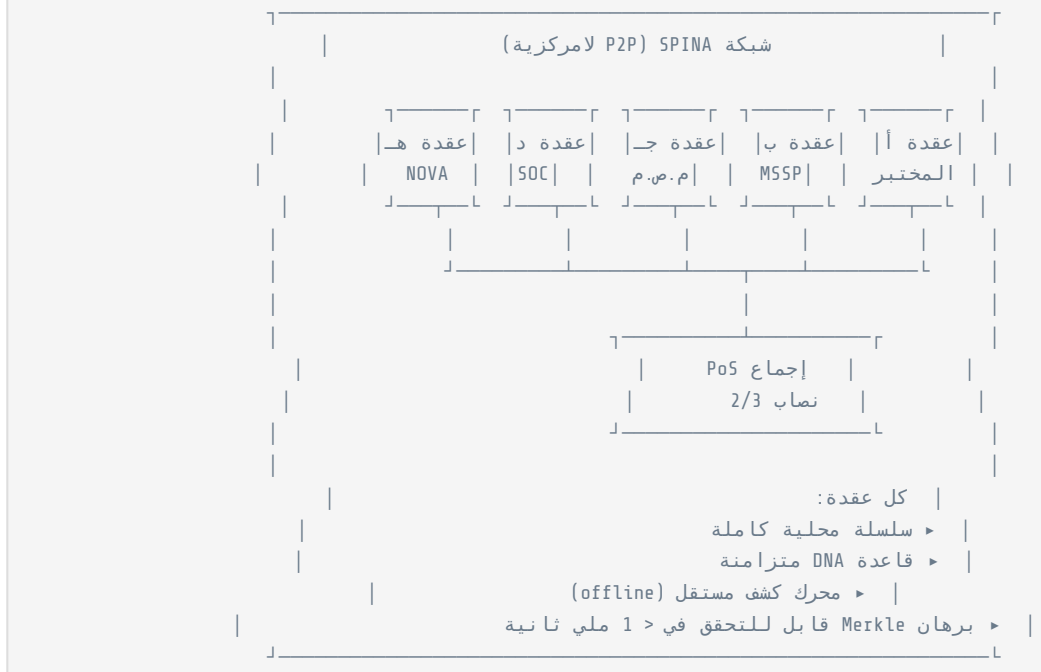
كل يوم، تُكتشف آلاف البرمجيات الخبيثة وتُحلل وتُحظر عبر العالم. كل SOC، وكل MSSP، وكل شركة تخوض هذا القتال بمعزل عن غيرها. برنامج فدية تم إحباطه في باريس لا يُحصّن مستشفى في طوكيو. توقيع يكتشفه متكافل NOVA في برلين لا يُشارك مع متكافل في ساو باولو — أو أسوأ من ذلك، يُشارك عبر قنوات احتكارية، بطيئة، مركزية، قابلة للفشل.

هذا هو **فقدان الذاكرة في الأمن السيبراني** . تنفق الصناعة 200 مليار دولار سنوياً لمكافحة تهديدات سبق لشخص ما، في مكان ما، أن هزمها. المعرفة موجودة — لكنها حبيسة الصوامع.

مبدأ

ما يتذكر ينجو. تهديد تمت رؤيته مرة واحدة يجب ألا يتمكن من الإضرار مجدداً — لا في أي مكان، ولا لأي شخص، وإلى الأبد.

٢. SPINA — الهندسة



شكل 1: الهندسة اللامركزية لـ SPINA

١.٢ كتلة SPINA

تعريف - كتلة SPINA

تحتوي كتلة SPINA B على:

- prev_hash — SHA-256 للكتلة السابقة
- timestamp — طابع زمني UTC معتمد
- payload — توقيع تهديد، أو تجزئة سلوك، أو تقرير تخدير
- merkle_root — جذر شجرة Merkle للتوقيعات النشطة
- validator_sig — توقيع Ed25519 لعقدة المُصدِّق

صلاحية B قابلة للتحقق من قبل أي عقدة بعملية تجزئة واحدة.

٢.٢ شجرة Merkle — التحقق بتعقيد O(log n)

قاعدة DNA الكاملة (أكثر من 25 ألف توقيع) مُهيكلة في شجرة Merkle. للتحقق من أن توقيعاً محدداً ينتمي إلى القاعدة، لا تحتاج العقدة إلى تنزيل 25 ألف مدخل — بل تتلقى برهان Merkle من $\log_2(25000) \approx 15$ تجزئة، أي حوالي 480 ثمانية (بايت). زمن التحقق أقل من 1 ملي ثانية.

٣.٢ إجماع تطوري

المرحلة	العقد	الإجماع	دور المختبر
الانطلاق	< 100	PoA (مُصدِّقات معروفة)	مُشغِّل رئيسي
النمو	100–1000	PoS هجين	مُصدِّق بين آخرين
النضج	+1000	PoS كامل	عقدة كغيرها

٣. SPINA كصالح عام

١.٣ رخصة MIT — صفر حواجز

يُنشر SPINA بموجب رخصة MIT. يمكن لأي شخص استخدامه، وتعديله، وإعادة توزيعه، ودمجه في منتجاته. لا إتاوات. لا عقود. لا إذن. إنها بنية تحتية عامة — مثل TCP/IP، مثل HTTP، مثل اللقاحات.

النموذج الاقتصادي

SPINA = مجاني. البروتوكول مشاع. كمياه الشرب. كالمعرفة.

NOVA = مدفوع. الكائن الحي الذي يستخدم SPINA — cockpit الجزيئي، Kenza، التطعيم، التخدير — هو منتج NOVA.

إنه نموذج Linux + Red Hat. HTTP + Google. البروتوكول حر. القيمة في التنفيذ.

٢.٣ لماذا اللامركزية

الذاكرة المركزية قابلة للفشل. قد يسقط مركز البيانات. قد تختفي الشركة. قد تفرض الدولة الرقابة. SPINA بلا مركز — وبالتالي بلا هدف، بلا نقطة فشل وحيدة، بلا سلطة يمكنها تغيير الحقيقة.

أنشأ المختبر البروتوكول. لكن يوم يزول المختبر، يستمر SPINA. لأن الذاكرة المناعية للبشرية الرقمية يجب ألا تعتمد على كيان واحد.

٤. التنفيذ التقني

```
مكدس SPINA (MVP) – أسبوعان)

P2P : libp2p (gossip protocol) ▸
الإجماع : PoA → PoS ▸
التوقيعات : Ed25519 ▸
التخزين : LevelDB + IPFS (للحمولات الكبيرة) ▸
Merkle : SHA-256, شجرة ثنائية ▸
API : REST (:5194) + gRPC ▸
اللغة : Python (MVP), Rust (v2) ▸

/opt/nova/spina/
├── chain.json          ← سلسلة خام (append-only)
├── merkle.db           ← SQLite (فهرس التوقيعات)
├── spina.py            ← المحرك الرئيسي
├── validators.yaml     ← مفاتيح NOVA Cores العمومية
└── api.py              ← REST :5194
```

شكل 2: المكدس التقني لـ SPINA MVP

عقدة SPINA كاملة تشغل أقل من 50 ميغابايت تخزين، وتستخدم أقل من 1% من CPU في النظام المستقر، وتستهلك حوالي 10 ميغابايت/يوم من النطاق الترددي. تعمل على Raspberry Pi، أو خادم قديم، أو في حاوية Docker.

٥. التكامل مع منظومة NOVA

شكل 3: دمج SPINA في خط الأنابيب المناعي لـ NOVA

٦. امتدادات طبيعية

التقارب الاستراتيجي. مع SPINA، يتقلص فضاء الاستراتيجيات الخبيثة مع كل تسجيل. بعد 10,000 برمجية خبيثة تم تخديرها، يتعرف النظام على برنامج الفدية عند أول حزمة — حتى قبل أن يبدأ أول إجراء ذي معنى. انظر الورقة 000 للنظرية الكاملة.

هوية المتكافلات. كل NOVA Core، وكل µNOVA يمتلك هوية على السلسلة قابلة للتحقق. مكافحة الانتحال تشفيرياً: لا يمكن لأي متكافل انتحال هوية آخر.

التدقيق والامتثال. ExpertCyber، ISO 27001، NIS2 — كل إجراء أمني مؤرخ وموقع في SPINA. يتحقق المدقق من السلامة ببرهان Merkle. صفر إمكانية تزوير.

٧. خاتمة

SPINA هو الجواب على مشكلة فقدان الذاكرة. الأمن السيبراني التقليدي يحارب نفس التهديدات آلاف المرات، بالتوازي، دون أن يشارك انتصاراته أبداً. SPINA يحوّل كل انتصار إلى مناعة جماعية.

إنه ليس منتجاً. إنه ذاكرة العالم الرقمي — مفتوحة، لامركزية، غير قابلة للتغيير.

> SPINA
>
> تهديد تمت رؤيته مرة واحدة. لا في أي مكان بعد الآن. ولا لأي شخص. وإلى الأبد.
>
> ما يتذكر ينجو.

المراجع

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

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

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

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

,H. TIKIJJA, « La Loi — Fondement Unifié des Organismes Numériques », 0DATA Lab [5]
.Papier 000, 2026

,H. TIKIJJA, « Le Système Immunitaire des Infrastructures », 0DATA Lab, Papier 005 [6]
.2026

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

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