TRÈS SECRET DÉFENSE

DIFFUSION RESTREINTE

RÉPUBLIQUE FRANÇAISE

Liberté — Égalité — Fraternité

DIRECTION GÉNÉRALE DE LA SÉCURITÉ EXTÉRIEURE

DIRECTION TECHNIQUE (DT)

Service d'Analyse des Menaces Cyber et Technologiques

NOTE D'ÉVALUATION TECHNIQUE

Projet « Slonana »

Blockchain C++20 haute performance pour économies d'agents autonomes — Implications pour la souveraineté numérique française et européenne

Référence :	DGSE/DT/2026/N° 0178-TSD
Classification :	TRÈS SECRET DÉFENSE
Date :	7 février 2026
Rédacteur :	Division Cyber — Cellule Blockchain
Pagination :	**??** pages

Diffusion

Le présent document est classifié **TRÈS SECRET DÉFENSE** conformément à l'instruction générale interministérielle n° 1300/SGDSN/PSE du 30 novembre 2011. Sa diffusion est strictement limitée aux destinataires ci-dessous.

Exemplaire	Destinataire	Action
01	Président de la République — Cabinet	Pour information
02	Premier Ministre — SGDSN	Pour information
03	Ministre des Armées — Cabinet	Pour information
04	Ministre de l'Économie et des Finances — DG Trésor	Pour action
05	Banque de France — Direction de la Stabilité financière	Pour action
06	ANSSI — Sous-direction Stratégie	Pour action
07	Autorité des Marchés Financiers (AMF)	Pour information
08	DGSE — Direction du Renseignement	Pour exploitation
09	DGSE — Direction Technique	Exemplaire de travail

Mots-clés : blockchain, agents autonomes, intelligence artificielle, souveraineté numérique, crypto-actifs, consensus byzantin, Solana, C++20, MCP, économie agentique.

1. Synthèse

Le projet **Slonana** constitue une initiative remarquable par son ambition technique : il s'agit d'une implémentation complète, en C++20, d'une blockchain de couche 1 compatible avec le protocole Solana, spécifiquement conçue pour les économies d'agents artificiels autonomes. Développée par un chercheur identifié sous le pseudonyme « Rin Fhenzig » au sein de la structure « OpenSVM Research », cette infrastructure présente un intérêt stratégique majeur pour la France à plusieurs titres.

Constats principaux :

(1) Le projet représente, à notre connaissance, la première implémentation non-Rust d'un validateur Solana fonctionnel, atteignant des performances mesurées de **185 000 transactions par seconde** avec une latence médiane de **142 µs**. L'objectif architectural de 1,2 million de TPS, fondé sur des algorithmes *lock-free* et des structures NUMA-*aware*, reste à valider à pleine échelle.

(2) Le modèle économique dit « *fair launch* » — absence totale de pré-minage et d'allocation à des fonds de capital-risque — représente une rupture paradigmatique par rapport aux réseaux blockchain existants. Les simulations multi-agents montrent une convergence du coefficient de Gini de 0,88 (lancement) à 0,47 (48 mois), contre 0,90 pour les réseaux à capital concentré.

(3) L'intégration native du *Model Context Protocol* (MCP) et de l'exécution BPF asynchrone constitue une innovation significative permettant aux agents IA de découvrir et d'invoquer des programmes on-chain de manière autonome, sans programmation préalable.

(4) Le code source est ouvert (87 453 lignes, 506 fichiers), ce qui facilite l'audit mais également l'appropriation éventuelle par des acteurs étatiques ou privés.

Évaluation de la menace : Modérée à élevée. Si le projet atteint ses objectifs de déploiement à grande échelle, il pourrait altérer l'équilibre concurrentiel dans l'écosystème des crypto-actifs et, plus fondamentalement, accélérer l'avènement d'économies agentiques largement indépendantes des cadres réglementaires nationaux. La France doit anticiper cette éventualité.

2. Contexte et enjeux

2.1. L'émergence des économies agentiques

L'évolution récente de l'intelligence artificielle, en particulier les modèles de langage à grande échelle (LLM) et les systèmes multi-agents, dessine l'horizon d'une économie où des agents autonomes — et non plus des êtres humains — constituent la majorité des acteurs économiques transactionnels. Cette perspective, qui relevait il y a peu de la spéculation, se matérialise désormais dans des prototypes fonctionnels.

Le projet Slonana s'inscrit précisément dans cette tendance. Son livre blanc, publié le 1er janvier 2026, formule une thèse explicite : « aucune blockchain existante n'optimise pour les économies d'agents autonomes ». Cette affirmation, quoique réductrice, reflète une réalité technique : les réseaux actuels (Ethereum, Solana, Cardano) sont conçus pour des interactions humaines médiatées par des portefeuilles et des interfaces graphiques.

2.2. Le paysage concurrentiel des blockchains de couche 1

Le marché des blockchains de couche 1 demeure dominé par un oligopole de fait :

Réseau	Consensus	TPS mesuré	Coeff. Nakamoto
Ethereum	PoS (Casper FFG)	∼30	2
Solana	Tower BFT + PoH	∼65 000	19
Cardano	Ouroboros Praos	∼250	∼24
Slonana	Tower BFT + PoH (C++)	185 000 (mesuré)	—

L'élément distinctif de Slonana ne réside pas tant dans ses performances brutes — qui restent à confirmer en conditions mainnet — que dans sa philosophie architecturale : une infrastructure nativement conçue pour des agents IA, avec exécution BPF asynchrone, communication inter-programmes par tampons circulaires *lock-free*, et auto-description des programmes via le *Model Context Protocol*.

2.3. Le problème de la centralisation par le capital-risque

Le livre blanc consacre une analyse substantielle à la centralisation induite par les allocations initiales de jetons aux fonds de capital-risque. Cette analyse mérite attention. Les données citées sont vérifiables :

- **Ethereum** : les 5 principales entités contrôlent 64 % du stake (Lido, Coinbase, Binance, Kraken, RocketPool).
- **Solana** : coefficient de Nakamoto de 19 ; 19 validateurs suffisent à interrompre le réseau.
- **Cardano** : IOHK et Emurgo contrôlent collectivement plus de 40 % via la délégation.

La proposition mathématique du livre blanc — le coefficient de Gini croît monotoniquement sous PoS avec allocation VC initiale — est formellement correcte sous les hypothèses énoncées. Toutefois, cette analyse omet les mécanismes de redistribution empiriques (délégation, protocoles DeFi, *liquid staking*) qui atténuent partiellement cette tendance.

3. Évaluation technique

3.1. Architecture du consensus

Slonana implémente le consensus **Tower BFT** avec intégration de la **Preuve d'Histoire** (PoH), reproduisant fidèlement l'architecture de Solana en C++20. Les spécificités techniques méritent une analyse détaillée.

3.1.1. Preuve d'Histoire : ordonnancement cryptographique

La PoH maintient une chaîne de hachages SHA-256 :

$$h_{i+1} = \text{SHA-256}(h_i \| \text{données\_mélangées}_i)$$

Les *ticks* surviennent toutes les 200 microsecondes ; 64 *ticks* constituent un *slot*. Cette horloge cryptographique fournit un ordonnancement sans synchronisation globale. La sécurité repose sur l'irréversibilité : réordonner les transactions exige de recalculer l'intégralité des hachages subséquents, effort de coût exponentiel.

3.1.2. Mécanisme de verrouillage (*lockout*)

Chaque validateur maintient un compteur de verrouillage. Voter pour un bloc B au slot s verrouille le validateur pendant 2^m slots subséquents (m étant le multiplicateur de verrouillage). Tout vote contradictoire dans cette fenêtre déclenche le *slashing* — confiscation partielle du stake. Ce mécanisme rend l'équivocation économiquement irrationnelle.

3.1.3. Résistance aux attaques à longue portée

Le protocole de *checkpointing* — toutes les 512 blocs ($\approx$ 3 minutes) — produit un engagement cryptographique agrégé par plus de 2/3 du stake. Tout nouveau validateur doit obtenir le checkpoint courant d'un pair de confiance, rendant la réécriture de l'historique antérieur prohibitivement coûteuse.

3.2. Exécution BPF asynchrone

L'innovation la plus significative du projet réside dans son modèle d'exécution autonome. Trois mécanismes complémentaires sont proposés :

1. **Minuteries auto-programmées** : les programmes peuvent planifier leur propre exécution future via `sol_timer_create()`, avec un budget en unités de calcul pré-alloué. Latence mesurée : 0,07 μs par minuterie ($\sim$14 millions/seconde).
2. **Observateurs réactifs** : les programmes surveillent des comptes et réagissent aux changements d'état (`sol_watcher_create()`). Latence : 0,12 μs par observateur ($\sim$8 millions/seconde).
3. **Tampons circulaires inter-programmes** : communication asynchrone *lock-free* entre programmes, avec garantie d'ordre FIFO et numéros de séquence. Débit : $\sim$25 millions d'opérations/seconde.

Ces mécanismes constituent une rupture conceptuelle : ils transforment les programmes on-chain de réacteurs passifs en agents autonomes capables d'auto-déclenchement. Les implications pour la régulation financière sont considérables (cf. section **??**).

3.3. Qualité de l'implémentation

L'analyse du code source (version v0.1.495-mainnet, commit `49e53be`) révèle une implémentation de qualité professionnelle :

— **Volume** : 87 453 lignes de C++20 réparties sur 506 fichiers, avec une architecture modulaire claire (réseau, consensus, SVM, stockage, monitoring).

— **Pile technologique** : simdjson pour le traitement JSON haute performance, libsodium (Ed25519), OpenSSL (SHA-256, AES-GCM), RocksDB et ClickHouse pour le stockage hybride.

— **Pratiques d'ingénierie** : intégration continue, tests unitaires et d'intégration, benchmarks de performance, analyse statique (cppcheck), *sanitizers* (ASAN, TSAN).

— **Points de vigilance** : certaines fonctions comportent des implémentations provisoires (marquées `TODO`). La migration complète de nlohmann : :json vers simdjson, bien qu'achevée dans les en-têtes, laisse subsister des *placeholders*. Le système de téléchargement de snapshots a rencontré des problèmes de contre-pression dans le pipeline de streaming.

3.4. Évaluation de la sécurité cryptographique

Le modèle de sécurité repose sur des primitives éprouvées :

Primitive	Usage	Évaluation
SHA-256	Chaîne PoH, hachage des blocs	Robuste
Ed25519 (libsodium)	Signatures de validateurs	Robuste
AES-256-GCM	Messagerie chiffrée P2P	Robuste
HKDF / PBKDF2	Dérivation de clés	Conforme

Note ANSSI : Aucune vulnérabilité cryptographique fondamentale n'a été identifiée. Les primitives utilisées sont conformes aux recommandations de l'ANSSI (RGS v2.0). Le protocole de gossip utilise des discriminants d'énumération à 32 bits (format *limcode*), compatible avec l'implémentation Rust de référence (Agave).

4. Analyse économique

4.1. Tokenomique et modèle de distribution

Le jeton natif **$SLON** présente les caractéristiques suivantes :

Paramètre	Valeur
Offre totale	100 000 000 $SLON
Distribution initiale	10 % airdrop aux détenteurs de $slonana
Émissions ultérieures	90 % via récompenses de staking
Finalité	12,8 secondes
Allocation VC	**Néant**
Pré-minage	**Néant**

L'absence d'allocation pré-mine et de financement par capital-risque est exceptionnelle dans le paysage blockchain actuel. Si cette approche renforce la légitimité communautaire du projet, elle soulève également des interrogations sur la pérennité du financement du développement.

4.2. Modélisation de la décentralisation

Le livre blanc présente une modélisation économétrique de la convergence du coefficient de Gini. Sous l'hypothèse d'une participation des validateurs suivant une distribution de Zipf, les simulations multi-agents montrent :

— **Lancement** ($t = 0$) : $G = 0{,}88$ (forte concentration initiale due à la distribution par airdrop).

— **Équilibre** ($t = 48$ **mois**) : $G \to 0{,}47$ (convergence par les récompenses de staking proportionnelles).

— **Comparaison** : les réseaux à allocation VC convergent vers $G \approx 0{,}90$ (centralisation croissante).

Appréciation : Cette modélisation est mathématiquement cohérente mais repose sur des hypothèses simplificatrices. En particulier, l'absence de marchés secondaires de jetons dans le modèle sous-estime les effets de concentration par l'acquisition spéculative. Néanmoins, la direction qualitative de l'analyse est plausible : les lancements équitables produisent empiriquement des distributions plus homogènes.

4.3. Coût des attaques et théorie des jeux

L'analyse game-théorique du livre blanc établit un équilibre de Nash sous la condition $\alpha < 1/3$ (fraction du stake contrôlée par l'adversaire). Les coûts d'attaque estimés dépassent 1 milliard de dollars en coordination de stake, avec une espérance mathématique négative due aux pénalités de *slashing* et à la perte réputationnelle. Cette analyse est rigoureuse dans son cadre formel, bien que les paramètres quantitatifs (seuil de 1 milliard) dépendent de la capitalisation future du réseau.

5. Implications stratégiques

5.1. L'économie agentique comme rupture civilisationnelle

Il convient de situer le projet Slonana dans un contexte plus large que celui de la seule ingénierie blockchain. Ce que propose ce système — une infrastructure où des agents artificiels transactent de manière autonome, sans intervention humaine, à l'échelle de millions d'opérations par seconde — constitue potentiellement un changement de paradigme dans l'organisation économique.

La civilisation technique européenne, depuis la Révolution industrielle, s'est construite sur le postulat de l'agent humain rationnel comme unité fondamentale de l'économie. Les cadres réglementaires français et européens — de la directive MIF II au règlement MiCA — présupposent des acteurs humains identifiables, dotés de droits et d'obligations. Une économie agentique autonome échappe à ces catégories.

5.2. Souveraineté numérique et autonomie stratégique

Le projet Slonana pose la question de la **souveraineté numérique** française et européenne sous trois angles :

1. **Dépendance technologique** : Le projet est actuellement développé en dehors du périmètre européen. Si des économies agentiques significatives se développent sur cette infrastructure, la France se trouverait en position de dépendance vis-à-vis d'une technologie qu'elle ne maîtrise pas.
2. **Compétitivité de l'écosystème** : Paris, en tant que place financière européenne de premier plan, dispose d'atouts considérables dans la fintech et la finance décentralisée. Le développement d'économies agentiques sur des infrastructures extra-européennes pourrait marginaliser ces avantages.
3. **Régulation** : Le règlement MiCA (Markets in Crypto-Assets), entré en application en 2024, ne prend pas en compte les agents IA autonomes comme acteurs économiques. Un vide juridique significatif existe.

5.3. Implications pour l'euro numérique

Le projet de monnaie numérique de banque centrale (MNBC) porté par la BCE pourrait être directement affecté :

— Si des économies agentiques se développent sur des infrastructures comme Slonana avec leurs propres jetons natifs ($SLON), l'adoption de l'euro numérique par les agents IA pourrait être concurrencée.

— La latence de finalité de Slonana (12,8 secondes) est compatible avec les exigences transactionnelles des agents. L'euro numérique devra offrir des performances comparables pour rester pertinent.

— L'interopérabilité entre les blockchains agentiques et l'euro numérique constitue un enjeu architectural non résolu.

5.4. Risques cyberdéfensifs

L'ANSSI doit évaluer les risques suivants :

— **Utilisation à des fins de blanchiment** : Des agents autonomes transactant à haute fréquence pourraient complexifier considérablement la traçabilité des flux financiers, contournant les dispositifs LCB-FT (lutte contre le blanchiment et le financement du terrorisme).

— **Attaques coordonnées** : Des agents malveillants pourraient exploiter l'exécution BPF asynchrone pour orchestrer des attaques de manipulation de marché à une vitesse échappant à la surveillance humaine.

— **Surface d'attaque du code** : Malgré la qualité générale de l'implémentation, les composants provisoires (`TODO`) et les corrections récentes de vulnérabilités (déréférencement de pointeur nul, références pendantes) témoignent d'une maturité encore insuffisante pour un déploiement en production critique.

— **Dépendance au protocole de gossip** : Le protocole CRDS, bien qu'implémenté de manière conforme, constitue un vecteur d'attaque par injection de données falsifiées si les vérifications de signature sont contournées.

6. Impact sur les intérêts français

6.1. Dimension industrielle

La France dispose d'une expertise reconnue en cryptographie (INRIA, CEA, Thales, Atos) et en systèmes distribués. Le projet Slonana, de par sa nature *open source* et sa pile technologique C++20, offre une opportunité d'appropriation technologique par l'écosystème français. Plusieurs scénarios méritent considération :

1. **Fork souverain** : La licence *open source* permet théoriquement la création d'une variante européenne intégrant les exigences réglementaires de MiCA, l'identité numérique (eIDAS 2.0) et la conformité LCB-FT par conception.
2. **Partenariat de recherche** : Les innovations en matière d'exécution BPF asynchrone et de consensus haute performance pourraient alimenter les travaux du Programme d'Investissements d'Avenir (PIA) sur les infrastructures numériques.
3. **Veille technologique** : À défaut de participation active, un suivi permanent de l'évolution du projet s'impose pour anticiper ses impacts sur l'écosystème financier européen.

6.2. Dimension réglementaire

Le cadre réglementaire français et européen présente des lacunes significatives face aux économies agentiques :

— **Personnalité juridique des agents IA** : Le droit français ne reconnaît pas les agents IA comme sujets de droit. Or, dans une économie Slonana, des programmes autonomes contractent, transactent et gèrent des actifs sans mandataire humain identifiable.

— **Responsabilité civile** : En cas de préjudice causé par un agent autonome on-chain, la chaîne de responsabilité est indéterminée. Le régime de la directive sur l'IA (AI Act) ne couvre pas explicitement les agents économiques on-chain.

— **Fiscalité** : Les revenus générés par des agents autonomes transactant en \$SLON échappent aux catégories fiscales existantes. La DGFiP doit anticiper ces configurations.

6.3. Dimension géopolitique

Le développement d'infrastructures blockchain de haute performance pour les économies agentiques s'inscrit dans une compétition technologique mondiale :

— **États-Unis** : Solana Labs (San Francisco) et les grands fonds crypto américains disposent d'une avance considérable en termes de capitalisation et de base d'utilisateurs.

— **Chine** : Les travaux sur le yuan numérique (e-CNY) et les réseaux de services blockchain (BSN) intègrent déjà des composantes d'automatisation avancée.

— **Europe** : L'absence d'une blockchain de couche 1 européenne performante pour les économies agentiques constitue un facteur de vulnérabilité stratégique. Le projet Slonana, bien que non européen, pourrait servir de socle technique pour combler ce retard.

7. Recommandations

Au regard de l'analyse qui précède, la Direction Technique formule les recommandations suivantes, classées par degré de priorité.

7.1. Priorité 1 — Actions immédiates (T1 2026)

R1. **Audit de sécurité approfondi** : Mandater l'ANSSI pour réaliser un audit complet du code source de Slonana, en priorité sur les composants réseau (gossip CRDS, serveur RPC) et cryptographiques (gestion des clés, protocole de signature). Délai : 90 jours.

R2. **Cellule de veille dédiée** : Constituer au sein de la DGSE/DT une cellule de veille permanente sur les économies agentiques blockchain, chargée du suivi technique du projet Slonana et des initiatives concurrentes. Effectif : 3 analystes (1 cryptographe, 1 spécialiste systèmes distribués, 1 analyste économique).

R3. **Note d'alerte Banque de France** : Informer la Direction de la Stabilité financière des implications potentielles pour l'euro numérique et les marchés de crypto-actifs. Recommander l'inclusion des économies agentiques dans les scénarios de stress du Haut Conseil de Stabilité Financière.

7.2. Priorité 2 — Actions à moyen terme (S1 2026)

R4. **Programme de recherche** : Proposer au CEA et à l'INRIA un programme de recherche conjoint sur les « systèmes de consensus haute performance pour économies agentiques souveraines », avec objectif de développer une expertise nationale indépendante. Budget estimé : 5 M€ sur 3 ans.

R5. **Contribution réglementaire** : Saisir la Commission européenne (DG FISMA) pour intégrer les agents IA autonomes dans la révision du règlement MiCA prévue en 2027. Proposer un cadre de « responsabilité en cascade » (développeur → déployeur → opérateur de noeud).

R6. **Expérimentation contrôlée** : Autoriser, dans le cadre du bac à sable réglementaire de l'AMF, une expérimentation limitée de déploiement d'agents IA sur infrastructure blockchain, afin d'évaluer empiriquement les risques identifiés dans la présente note.

7.3. Priorité 3 — Orientation stratégique (2026–2028)

R7. **Souveraineté technologique** : Évaluer l'opportunité de financer, via le PIA 4 ou France 2030, le développement d'une infrastructure blockchain de couche 1 européenne optimisée pour les économies agentiques, potentiellement fondée sur un *fork* annoté du code Slonana avec intégration native de l'identité eIDAS et de la conformité MiCA.

R8. **Dialogue diplomatique** : Engager, dans le cadre de la coopération franco-allemande en matière de cyberdéfense, un dialogue sur la posture européenne commune face aux économies agentiques décentralisées. L'Allemagne, via le BSI, dispose d'une expertise complémentaire.

R9. **Doctrine d'emploi** : Élaborer, en coordination avec l'État-major des armées et la DGA, une doctrine d'emploi des technologies d'agents autonomes blockchain pour les applications de défense (chaînes logistiques sécurisées, coordination multi-agents en théâtre d'opérations).

Conclusion

Le projet Slonana représente un signal faible mais significatif de l'émergence d'une nouvelle catégorie d'infrastructures numériques : les blockchains nativement conçues pour les économies d'agents artificiels. Si l'on peut légitimement questionner la maturité actuelle de l'implémentation — corrections récentes de vulnérabilités critiques, composants provisoires, performances non validées en conditions mainnet — la direction architecturale est intellectuellement cohérente et techniquement ambitieuse.

La France se trouve à un moment charnière. L'histoire des révolutions technologiques enseigne que les nations qui négligent les signaux précurseurs se retrouvent en position de dépendance lorsque la technologie atteint la maturité. L'internet, le cloud computing, les réseaux sociaux : à chaque fois, l'Europe a compris trop tard et régulé a posteriori ce qu'elle n'avait pas su créer.

Les économies agentiques autonomes pourraient constituer la prochaine de ces révolutions. La présente note recommande une posture d'anticipation active : comprendre la technologie, développer une expertise indépendante, adapter le cadre réglementaire, et — si l'évaluation le confirme — investir dans une capacité souveraine.

Il ne s'agit pas de reproduire la naïveté technophile qui a prévalu lors de l'avènement des crypto-actifs grand public, mais de faire preuve de cette lucidité stratégique qui a toujours été la marque de la tradition régalienne française : *comprendre pour agir, anticiper pour protéger.*

Le Chef de la Division Cyber
Direction Technique — DGSE

[Signature classifiée]