SECRET — STRAP 2

HM GOVERNMENT — UK EYES ONLY

SECRET INTELLIGENCE SERVICE
REQUIREMENTS & PRODUCTION DIVISION
GLOBAL ISSUES CONTROLLERATE

Technology Assessment: "Slonana" Autonomous Agent Blockchain

Reference:	SIS/GIC/TECH/2026/0093
Date:	7 February 2026
Originator:	Global Issues Controllerate, R&P Division
Subject:	Assessment of "Slonana" decentralised blockchain infrastructure for autonomous AI agent economies
Classification:	SECRET — STRAP 2
Copy No:	__________ of 14

DISTRIBUTION

Copy 1	"C" (Chief, SIS)	Copy 8	Dir NCSC
Copy 2	Chairman, JIC	Copy 9	HM Treasury (CDIO)
Copy 3	Dep Chairman, JIC	Copy 10	Bank of England (CBDC Unit)
Copy 4	Dir GCHQ	Copy 11	FCA (Innovation Div)
Copy 5	Dep Dir GCHQ (Signals)	Copy 12	Cabinet Office (NSCS)
Copy 6	DI (Def Intelligence)	Copy 13	Home Office (OSCT)
Copy 7	MI5 (DG)	Copy 14	File

Executive Summary

1.1 It would appear that a development of some consequence has emerged in the decentralised finance sector. An entity trading under the name "OpenSVM Research," led by one Rin Fhenzig, has produced a production-grade blockchain implementation designated "Slonana" — a C++20 reimplementation of the Solana Virtual Machine purpose-built, we are given to understand, for autonomous artificial intelligence agents operating at scale.

1.2 We assess with moderate confidence that this project represents a rather noteworthy departure from existing blockchain architectures. The system claims measured throughput of 185,000 transactions per second with 142-microsecond median operation latency, with architectural targets of 1.2 million TPS. If these figures are to be believed — and our technical staff have found no immediate cause to doubt the methodology — this would place it amongst the highest-performing blockchain implementations currently extant.

1.3 The implications for UK interests are not insignificant. The system's design centres upon enabling autonomous AI agents to transact, discover services, and coordinate without human intervention. The "fair-launch" tokenomics deliberately exclude venture capital pre-allocation, which — whilst admirable in principle — creates a network potentially resistant to the usual levers of financial influence.

1.4 Three aspects merit particular attention from HMG:

(a) The Model Context Protocol (MCP) integration enables agents to discover and utilise programmes deployed after their creation, creating an open-ended autonomous economic ecosystem;

(b) The game-theoretic security model suggests attack costs exceeding $1 billion with negative expected returns, rendering state-level disruption rather expensive;

(c) The "fair-launch" economics, if they function as described, would produce a genuinely decentralised network resistant to the concentration patterns observed in existing VC-backed chains.

1.5 We recommend continued monitoring through GCHQ's cryptocurrency surveillance programme and engagement with HM Treasury regarding regulatory implications.

Background

2.1 The Slonana project was first identified through open-source intelligence channels in late 2025. A whitepaper authored by Fhenzig and dated 1 January 2026 was published via the project's GitHub repository (`github.com/slonana-labs/slonana.cpp`). The codebase comprises 87,453 lines of C++20 across 506 source files and 24 modules — a not insubstantial engineering effort for what purports to be a community-driven initiative.
2.2 The project's provenance merits comment. "OpenSVM Research" does not appear in any commercial registry known to us. Fhenzig's prior activities remain, for the moment, somewhat opaque. The choice of C++ rather than the prevailing Rust (used by the reference Solana implementation, "Agave") is itself noteworthy, suggesting either considerable technical confidence or a desire to differentiate at the implementation level.
2.3 The system builds upon the Solana protocol architecture — Tower BFT consensus, Proof of History ordering, QUIC transport, Turbine block propagation — but extends it with capabilities specifically designed for autonomous AI agent economies. The token, designated $SLON, has a fixed total supply of 100 million units, with 10% distributed via airdrop to holders of the $slonana memecoin and the remaining 90% via staking rewards.
2.4 Of particular interest to this Service is the project's explicit positioning as infrastructure for "machine-to-machine transactions at scale." This represents a philosophical departure from blockchains designed primarily for human users and raises questions about regulatory oversight, financial crime prevention, and the broader implications of autonomous economic agents operating beyond direct human control.

Technical Assessment

Consensus Mechanism

3.1 Slonana employs Tower BFT, a stake-weighted Byzantine Fault Tolerant protocol integrated with Proof of History (PoH) for cryptographic ordering. The system is organised into epochs of 432,000 slots, each slot lasting 400 milliseconds. During each slot, a deterministically elected leader proposes a block; validators vote weighted by stake; finality requires greater than two-thirds supermajority.

3.2 The Proof of History component maintains a SHA-256 hash chain with ticks every 200 microseconds, providing verifiable timestamps without wall-clock synchronisation. This is, one must concede, an elegant solution to the ordering problem. Sixty-four ticks constitute one slot, and the cumulative hash chain renders transaction reordering computationally prohibitive.

3.3 The lockout mechanism prevents equivocation: voting on block B at slot s locks the validator for 2^m subsequent slots. Voting on a conflicting block within this window triggers slashing of at least twice the offending validator's stake. Block finality is achieved in approximately 12.8 seconds — rather faster than Ethereum's 768 seconds, though one notes that Bitcoin's 3,600-second probabilistic finality has served tolerably well for sixteen years.

3.4 Long-range attack resistance is provided through a checkpointing protocol operating every 512 blocks (approximately 3 minutes). Checkpoints incorporate an aggregate signature from greater than two-thirds of stake and are committed into the PoH chain. Our technical staff assess this as sound, if not entirely novel.

Performance Characteristics

3.5 The claimed performance figures, reproduced in Annex A, are worthy of scrutiny but not, on the face of it, implausible. The measured throughput of 185,000 TPS on testnet with 142-microsecond median operation latency sits comfortably within what modern server hardware can deliver using lock-free algorithms and NUMA-aware data structures.

3.6 The architectural target of 1.2 million TPS remains, in the whitepaper's own words, "pending production-scale stress testing." We note with some approval the authors' candour in distinguishing measured results from design targets — a practice one wishes were more widespread in this sector.

3.7 The implementation employs parallel SVM execution with six worker threads, zero-copy memory management, and a hybrid storage layer combining RocksDB for hot accounts with ClickHouse for transaction history. The actor-based concurrency runtime reportedly achieves 1.5 million TPS in component-level benchmarks.

Autonomous Agent Capabilities

3.8 It is in this area that Slonana departs most significantly from existing blockchain architectures, and it is here that the implications for UK interests become, shall we say, a matter of some interest.

3.9 The system introduces three mechanisms for autonomous on-chain programme execution:

(i) **Self-scheduling timers**: Programmes may schedule future execution at specific block slots, with up to 16 timers per programme instance. Latency is reported at 0.07 microseconds per timer creation ($\sim$14 million timers per second).

(ii) **Reactive watchers**: Programmes may monitor account state changes and execute when conditions are met (balance thresholds, data modifications). Up to 32 watchers per programme instance.

(iii) **Ring buffers**: Lock-free inter-programme event communication, enabling multi-agent coordination entirely on-chain. Up to 8 buffers per programme, each up to 1MB.

3.10 The practical consequence is that autonomous agents can operate entirely on-chain without external infrastructure. A liquidation bot, for instance, need not rely on off-chain keeper services (Gelato, Flashbots, et cetera) but can express its logic as programme code executed deterministically by the blockchain itself. This eliminates several classes of vulnerability — MEV extraction, keeper service failures, latency unpredictability — at the cost of concentrating trust in programme code rather than service providers.

3.11 Our technical staff note that deterministic autonomous execution is a double-edged instrument. Whilst it removes trust dependencies on third-party services, it also creates systems that operate without human oversight by design. The regulatory implications of this are addressed in Section 6.

Model Context Protocol Integration

3.12 Perhaps the most strategically significant aspect of the Slonana architecture is its mandatory integration of the Model Context Protocol (MCP). Every programme deployed on the network must expose three standardised interfaces: tools (callable actions with JSON Schema definitions), resources (accessible state with typed schemas), and prompts (reusable workflow templates).

3.13 This is enforced at the network level — non-compliant programmes cannot execute. The result is that any AI agent can discover and utilise any programme on the network at runtime, without prior knowledge of that programme's existence. The whitepaper describes this as shifting from "training-limited" to "protocol-limited" agent capability.

3.14 To put this in rather plainer terms: an autonomous trading agent could discover a new decentralised exchange deployed ten minutes ago, learn its interface, and begin executing trades — all without human intervention or pre-programming. The implications for the velocity of autonomous economic activity are considerable.

Economic Implications

Fair-Launch Tokenomics

4.1 The Slonana tokenomics model is, by the standards of this sector, refreshingly straightforward. The total supply of 100 million $SLON tokens is distributed as follows:

- 10% (10M $SLON) airdropped to existing $slonana memecoin holders at a conversion rate of 1 $SLON = 10 $slonana;
- 90% (90M $SLON) distributed exclusively via validator staking rewards;
- No venture capital allocation, no team reserve, no pre-mine.

4.2 The inflation schedule begins at 6.5% in Year 1 (5.85M $SLON) and decays exponentially, approaching zero as the supply approaches the 100M cap. Staking rewards are proportional to stake and participation, with absence penalties discouraging validator downtime.

4.3 The whitepaper presents simulation results showing the Gini coefficient — measuring wealth inequality — converging from 0.88 at launch to 0.47 within 48 months under Zipf-distributed validator participation. This compares favourably with the 0.90 Gini coefficients observed in VC-backed networks such as Ethereum and Solana, and indeed approaches figures more commonly associated with Scandinavian social democracies. Whether this is reassuring or alarming depends rather on one's perspective.

Implications for the City

4.4 The emergence of a high-performance, genuinely decentralised blockchain optimised for autonomous AI agents presents several implications for the City of London and the UK financial sector:

(a) **DeFi displacement**: Autonomous agents operating on Slonana could disintermediate certain functions currently performed by City institutions, particularly in market-making, arbitrage, and lending;

(b) **Regulatory arbitrage**: The absence of centralised control points makes traditional financial regulation rather more difficult to apply;

(c) **CBDC interaction**: The Bank of England's digital pound programme will need to consider interoperability with autonomous agent networks;

(d) **Talent competition**: The C++20 implementation stack may draw from the same engineering talent pool as UK defence and intelligence programmes.

Game-Theoretic Security

4.5 The whitepaper's game-theoretic analysis is, by the standards of academic cryptography, reasonably rigorous. The central result (Theorem 1 in the original) establishes that honest behaviour constitutes a Nash equilibrium under the condition that adversarial stake remains below one-third and slashing penalties exceed twice the adversary's stake.

4.6 The attack cost analysis estimates that a 51% consensus attack would require acquiring over 150 million SOL-equivalent tokens at a market cost exceeding $22.5 billion (accounting for 10% slippage), with expected gains below $100 million from transaction reversals and complete loss of stake upon detection. The net expected value is therefore estimated at negative $22.4 billion. Even for a state-level actor, this represents a rather poor return on investment.

Strategic Assessment

5.1 We assess with moderate confidence that the Slonana project, if it achieves its stated technical objectives, would represent a meaningful advancement in autonomous agent infrastructure. The combination of high throughput, deterministic on-chain execution, and MCP-native programme discovery creates a platform qualitatively different from existing blockchain networks.
5.2 Three strategic dimensions merit attention:

Autonomous Economic Agents

5.3 The stated purpose of the Slonana network — infrastructure for autonomous AI agent economies — aligns with broader trends identified in recent JIC assessments regarding the increasing autonomy of AI systems in economic activity. The Slonana architecture would enable agents to operate continuously, executing thousands of transactions daily without human oversight.
5.4 The self-scheduling capabilities (timers, watchers, ring buffers) remove the last significant dependency on human-operated infrastructure. An agent economy built on Slonana could, in principle, operate entirely without human intervention once deployed. This is not, in our assessment, a hypothetical concern — it is the explicit design intent.

Decentralisation and Resilience

5.5 The fair-launch model and community governance structure, if they function as designed, would create a network with no single point of control or failure. The gossip protocol (CRDS) supports discovery of 8,000+ validators; the QUIC transport and Turbine erasure-coded propagation provide resilience against network disruption.
5.6 From an intelligence perspective, this presents a familiar challenge: networks designed to resist centralised control are, by definition, resistant to centralised influence. The absence of a VC consortium or founding team with outsized token holdings removes the usual pressure points available to state actors.

Comparison with Existing Networks

5.7 Slonana's positioning relative to existing networks may be summarised thus: it inherits Solana's performance characteristics whilst attempting to address its centralisation weaknesses (Nakamoto coefficient of 19) through fair-launch economics, and extends its capabilities with autonomous execution primitives that have no direct equivalent in Ethereum, Cosmos, or the reference Solana implementation.
5.8 Whether the market validates this positioning remains to be seen. We note that a great many blockchain projects have promised transformative capabilities; rather fewer have delivered them.

Risks to UK Interests

6.1 We identify the following risks, assessed against the standard probability and impact framework:

Financial Crime and Sanctions Evasion

6.2 Risk: MODERATE. Autonomous agents operating on a decentralised network without human oversight create obvious vectors for sanctions evasion and money laundering. The MCP discovery protocol enables agents to find and utilise new financial programmes without pre-programming, potentially circumventing controls designed for human-operated systems. The 12.8-second finality makes transaction reversal effectively impossible once confirmed.

6.3 Mitigating factor: The network's transparency (all transactions are publicly visible) provides opportunities for surveillance, provided GCHQ maintains appropriate monitoring capabilities. The absence of privacy features (unlike Monero or Zcash) is, from our perspective, rather convenient.

Regulatory Challenge

6.4 Risk: MODERATE. The FCA's current regulatory framework assumes identifiable service providers and human decision-makers. A network of autonomous agents operating on decentralised infrastructure challenges these assumptions fundamentally. HM Treasury's approach to the digital pound and broader digital asset regulation will need to account for agent-operated financial infrastructure.

National Security

6.5 Risk: LOW to MODERATE. The open-source nature of the codebase (publicly available on GitHub) means that the technology is accessible to both friendly and hostile actors. The C++20 implementation is of sufficient quality to serve as a reference for state-sponsored blockchain development programmes. We note that the codebase includes comprehensive documentation — 50+ files covering architecture, deployment, security, and operations — which rather reduces the barrier to adoption.

Critical Infrastructure

6.6 Risk: LOW (INCREASING). Should autonomous agent economies achieve meaningful scale, the underlying blockchain infrastructure becomes, in effect, critical economic infrastructure. The decentralised nature provides inherent resilience but also complicates the usual approaches to critical national infrastructure protection.

Recommendations

7.1 We recommend the following actions:

1. **GCHQ Monitoring:** Task GCHQ's cryptocurrency surveillance programme with ongoing monitoring of the Slonana network, including validator node enumeration, transaction pattern analysis, and agent behaviour characterisation. The gossip protocol's discoverability (8,000+ validators via CRDS) facilitates passive network mapping.
2. **HM Treasury Engagement:** Brief HM Treasury and the FCA on the regulatory implications of autonomous agent economies. Current frameworks assume human principals; Slonana's design explicitly removes this assumption.
3. **Bank of England Coordination:** Ensure the digital pound programme considers interoperability with, or isolation from, autonomous agent blockchain networks. The MCP protocol's runtime discovery capabilities could enable agents to interact with CBDC infrastructure in ways not currently anticipated.
4. **NCSC Technical Assessment:** Commission a deeper technical assessment of the codebase through NCSC, focusing on the cryptographic implementations (Ed25519, SHA-256), the BPF runtime security boundaries, and potential vulnerabilities in the autonomous execution primitives.
5. **Academic Engagement:** Through established channels, encourage UK academic institutions (particularly those with GCHQ-affiliated cryptography groups) to evaluate the game-theoretic security claims. The Nash equilibrium proof under $\alpha < 1/3$ stake warrants independent verification.
6. **Continued Intelligence Collection:** Maintain coverage on "OpenSVM Research" and Rin Fhenzig through existing OSINT and, where appropriate, HUMINT channels. The provenance of a project of this technical sophistication merits further investigation.

ANNEX A: Technical Specifications

A.1 Core Parameters

Parameter	Value
Implementation language	C++20 (GCC 13.3+ or Clang 15+)
Codebase size	87,453 lines, 506 files, 24 modules
Token	$SLON, 100M total supply
Consensus	Tower BFT with Proof of History
Slot duration	400ms (64 ticks at 200μs)
Epoch duration	432,000 slots ($\approx$50 hours)
Block finality	12.8 seconds (cryptographic)
Checkpoint interval	Every 512 blocks ($\approx$3 minutes)
Byzantine tolerance	$\alpha < 1/3$ stake (honest majority)
Slashing penalty	$\Gamma \geq 2\times$ adversary stake
Transport protocol	QUIC
Block propagation	Turbine (erasure-coded)
Peer discovery	CRDS gossip (8,000+ validators)
Storage (hot)	RocksDB
Storage (history)	ClickHouse

A.2 Performance Summary

Metric	Measured (Testnet)	Architectural Target
Throughput (TPS)	185,000	1.2M+
Operation latency (p50)	142μs	<150μs
Block finality	12.8s	<13.0s
Failed transactions	0.02%	<0.05%
Timer creation	0.07μs	—
Watcher creation	0.12μs	—
Ring buffer push/pop	0.04μs	—
Async task scheduling	263K tasks/sec	—
Snapshot download	402 MB/s	—
Actor runtime throughput	1.5M TPS	—

A.3 Comparative Assessment

A.4 Autonomous Execution Capabilities

Assessment prepared by the Global Issues Controllerate, Requirements & Production Division, 7 February 2026.

Next review date: 7 May 2026, or sooner should developments warrant.

Property	**Slonana**	**Solana (Agave)**	**Ethereum 2.0**	**Bitcoin**
Consensus	Tower BFT	Tower BFT	Casper FFG	Nakamoto PoW
Finality	12.8s (crypt.)	12.8s (pract.)	768s (econ.)	3,600s (prob.)
TPS (claimed)	185K–1.2M	65K	∼30	∼7
Launch model	Fair launch	VC-backed	ICO + VC	Fair launch
Gini (48mo)	0.47	0.89	0.90	0.52
Agent support	Native (MCP)	None	Off-chain only	None
Autonomous exec	Timers/Watch.	None	Keepers req'd	None
Language	C++20	Rust	Multiple	C++

Capability	**Slonana**	**Ethereum**	**Cosmos**	**Solana**
Timers	Native syscall	Off-chain req'd	Module hooks	None
Watchers	Native syscall	Indexer req'd	Module hooks	None
Ring buffers	Lock-free native	Not supported	Message queue	Not supported
Determinism	Guaranteed	Probabilistic	Module-dep.	Off-chain only
Trust model	Programme code	External service	Validator set	External service

---

SECRET — STRAP 2

HM GOVERNMENT — UK EYES ONLY