FLARESIGNAL

FLSG DEVELOPMENT ROADMAP

From ecosystem intelligence platform to autonomous machine-access protocol

ROADMAP / TECHNICAL DEVELOPMENT STATE v0.9

2 November 2026

ROADMAP PRINCIPLE

No artificial launch dates. Each FLSG phase opens only when the preceding product, commerce, specification, security, funding, legal, liquidity and price-authority evidence is satisfied.

ESTABLISHED SUBSTRATE

Independent FLR/SGB ecosystem intelligence and canonical machine interfaces

CURRENT FRONTIER

Production convergence plus Base mainnet machine-commerce validation

PROTOCOL STATE

FLSG V1 implementation specification and assurance readiness substantially defined; production evidence/configuration remains gated

ORIGINS

1. Product foundation before protocol economics

FlareSignal began as an independent intelligence platform for the Flare and Songbird ecosystems. The machine-access economy is proposed downstream of an operating product, not as a token launched in search of utility.

PRODUCTION INTELLIGENCE FOUNDATION

- Equal FLR/SGB coverage with XRPFi, Firelight/FIRE and third-party protocol context.
- Storage-transparent FS_Data_Core truth boundary shared by public, Pro and machine consumers.
- Network, Economy, XRPFi, Wallet + Market, Burn, Capital Flow, Events, Yield and FIRE intelligence.
- Eleven Sig-Metric families spanning execution, liquidity, policy transmission, capital character, demand persistence, distribution, utility, concentration, protocol flows, derivatives and composite regimes.
- Professional charting/workstation and shared Signal Lens presentation system.
- REST/OpenAPI, MCP and A2A interfaces with product definitions, metering, entitlement and idempotency foundations.

THE SEQUENCING DECISION

The intelligence stack, evidence architecture and machine-product surface came first. FLSG is proposed only because that substrate creates a specific machine-access and capacity-management use case.

COMPLETE

Canonical data plane

Official and chain evidence resolves through the same canonical truth boundary for humans and machines.

COMPLETE

Machine interface plane

Discovery, product contracts, metering and entitlement primitives already exist independently of FLSG.

COMPLETE

Payment substrate

PayChain provides deterministic crypto-payment verification and purchase activation before token economics.

CURRENT POSITION

2. Current technical state

FLSG remains a research architecture downstream of an operating FlareSignal intelligence stack. Current execution is focused on production convergence and final proof of autonomous paid machine commerce. Phase 3 has advanced into implementation specification and assurance readiness, while production evidence and deployment configuration remain gated.

PROGRAMME LAYER	STATE	TECHNICAL SCOPE	GATE CONDITION
Canonical intelligence stack	COMPLETE	FS_Data_Core, public/Pro intelligence, Sig-Metrics and machine interfaces.	Independent product substrate exists without FLSG.
Production convergence	ACTIVE	Source authority, freshness, retained history, shared component parity and release certification.	Production baseline is stable for machine-commerce activation.
Machine commerce substrate	PRODUCTION GATE	PayChain, machine products and Base Sepolia x402 proof complete; Base mainnet USDC canary pending.	Production Base settlement and delivery proof closes Phase 2.
FLSG protocol specification	IMPLEMENTATION SPEC DEFINED	V1 monetary, customer-property, access and escrow behavior specified; reference modelling, formal property definitions, economic attack modelling, release-security preparation and transparency design prepared.	Measured production configuration plus production price/deployment identifiers remain gated.
Coston2 immutable kernel	FUTURE GATE	Minimal token/access/escrow/burn/liquidity contracts on Flare testnet.	Phase 3 explicit close and Phase 2 evidence precede implementation.

PHASE 3 ASSURANCE READINESS NOW PREPARED

- Monetary and customer-property invariants plus deterministic access/escrow behavior are implementation-specified.
- Authority and signing-security architecture is defined without creating an operator path to customer principal.
- An executable V1 reference model and formal property set are prepared for differential verification against later Solidity.
- Economic attack modelling and an audit-ready security/release pipeline are prepared before contract implementation.
- Public transparency and external-assurance/grant readiness are designed while operational secrets remain private.

FULL SEQUENCE

3. Protocol development sequence

The programme advances by technical dependency and evidence. A phase opens when its preceding validation gate is satisfied, not because a calendar date has arrived.

PHASE 0

Canonical Intelligence & Payment Substrate

COMPLETE

PHASE 1

Production Readiness & Canonical Convergence

ACTIVE

PHASE 2

Machine Commerce & PayChain Proof

PRODUCTION GATE

PHASE 3

Protocol Specification & Assurance Readiness

IMPLEMENTATION SPEC DEFINED

PHASE 4

PHASE 5

Adversarial Validation & Reproducible Security

GATED

PHASE 6

External Assurance & Mainnet Genesis

GATED

PHASE 7

Market Bootstrap, Price Authority & SIGNAL Access

GATED

PHASE 8

Usage-Derived Burn Activation

GATED

PHASE 9

CURRENT EXECUTION FRONTIER

Phase 1 remains the active production-convergence frontier. Phase 2 has a proven substrate and waits on Base mainnet production settlement. Phase 3 now has a substantially defined V1 implementation specification and assurance-readiness package, while measured production configuration remains gated. Phases 4-9 remain implementation, security, legal, market and economic gates.

DETAILED ROADMAP

4. Foundation and production convergence

PHASE 0

COMPLETE

Canonical Intelligence & Payment Substrate

Canonical FlareSignal data, machine interfaces and payment infrastructure operate independently of FLSG economics.

PROTOCOL / INFRASTRUCTURE DELIVERABLES

- FS_Data_Core storage-transparent canonical truth boundary across public, Pro and machine consumers.
- Public/Pro intelligence, Sig-Metrics and retained-history surfaces backed by official/chain evidence.
- REST/OpenAPI, MCP and A2A interfaces with metering, entitlement and idempotency foundations.
- PayChain crypto-payment substrate with deterministic payment verification and purchase activation.
- Data-minimised ordinary account boundary: email + password only.

VALIDATION GATE Canonical intelligence, machine-access and payment infrastructure operate without dependency on FLSG.

PHASE 1

ACTIVE

Production Readiness & Canonical Convergence

Converge every production surface on the established truth architecture, retention semantics and shared component standards.

- Complete customer-surface source, freshness, history and canonical-owner verification.
- Prove repeated live/cycling values consume shared canonical clocks.
- Close remaining responsive, light-mode and shared-component parity defects without redesigning locked surfaces.
- Enforce immediate-parent release scope, executable runtime safety and byte-level regression certification.
- Freeze a production-ready product baseline for machine-commerce proof.

VALIDATION GATE No known customer-facing truth, source, history or interface inconsistency remains in the production baseline.

DETAILED ROADMAP

5. Machine commerce and Phase 3 readiness

PHASE 2

4 / 6 VERIFIED

Machine Commerce & PayChain Proof

The machine-commerce substrate is proven through PayChain and Base Sepolia. Production closure now depends on Base mainnet settlement and a real-USDC canary.

VERIFIED	PayChain deterministic payment verification, signed receipt and entitlement activation.
VERIFIED	Machine discovery, OpenAPI, MCP, A2A, six product contracts, delegated execution, metering and idempotency foundations.
VERIFIED	x402 Base Sepolia: HTTP 402 challenge, signed retry, facilitator verification/settlement, receipt, entitlement, metering and audit linkage.
VERIFIED	Deterministic settlement/replay foundations proven in the canary path.
IN VALIDATION	Base mainnet production settlement configuration, payment destination, pricing/preflight and real-USDC canary.
GATED	Final production autonomous purchase, delivery/output verification, settlement/refund, ledger and replay evidence.

PHASE 3

6 / 7 MILESTONES

Protocol Specification & Assurance Readiness

V1 monetary, customer-property, access and escrow behavior is substantially specified. Security-assurance preparation has also advanced. Production evidence and deployment configuration remain gated before Phase 3 closes.

DEFINED	Monetary and customer-property invariants, including fixed supply, FLR gas and non-discretionary customer principal.
DEFINED	SIGNAL Access and machine-order escrow lifecycles with immutable customer rights and deterministic settlement/refund boundaries.
DEFINED	Flare-native pricing/trust, Service Policy measurement and isolated evidence architecture without a parallel site truth system.
PREPARED	Authority/key-security architecture plus an executable V1 reference model for implementation and differential testing.
PREPARED	Formal property definitions, economic attack modelling and an audit-ready security/release pipeline.
PREPARED	Public transparency design and external-assurance/grant readiness for later independent review.
GATED	Measured production demand, production price/deployment identifiers and explicit Phase 3 closure before Phase 4 opens.

DETAILED ROADMAP

6. Immutable kernel and adversarial assurance

PHASE 4

FUTURE GATE

Coston2 Immutable Kernel

Implement the smallest security-critical FLSG protocol kernel on Flare Coston2 using audited primitives wherever possible.

- FLSGToken: fixed genesis supply and native burn with no owner monetary controls.
- SIGNALAccessLock: principal, expiry, beneficiary integrity and entitlement view with no admin principal path.
- AccessSchedule: epoch-based economic requirements that cannot alter existing locks.
- MachineOrderEscrow: deterministic funded -> fulfilled -> settled OR refunded state machine.
- UsageBurnVault, liquidity and vesting controls with narrow capabilities and no generic execution surface.

VALIDATION GATE Complete lifecycle executes on Coston2 with test assets while customer principal remains non-discretionary.

PHASE 5

FUTURE GATE

Adversarial Validation & Reproducible Security

Establish evidence that critical invariants survive hostile call sequences, malicious assets, compromised agents and build-chain failure.

- Stateful fuzzing across caller, amount, timing and transaction-sequence space.
- Mutation testing that intentionally weakens security checks and requires tests to detect the change.
- Property-directed AI red-team against monetary, custody, replay, burn-isolation and privacy invariants.
- Formal verification of highest-value invariants using independent methods where practical.
- Reproducible build/bytecode verification, canary limits and data-minimisation validation.
- Non-destructive external funding/grant routes for specialist assurance.

VALIDATION GATE Critical invariants survive independent adversarial methods and reproducible deployment evidence is available.

DETAILED ROADMAP

7. Mainnet assurance and price authority

PHASE 6

FUTURE GATE

External Assurance & Mainnet Genesis

Cross the Mainnet boundary only after independent security assurance, legal review and final genesis engineering.

- Independent smart-contract audit, remediation and remediation verification.
- UK legal/regulatory review of token distribution, burn, liquidity and machine-access structure.
- Final immutable genesis, treasury/founder vesting and purpose-bound security vaults.
- Public price-discovery mechanism subject to legal approval and anti-manipulation constraints.
- Protocol-owned liquidity plus verified source, bytecode hashes and public authority matrix.

VALIDATION GATE Mainnet contracts, launch mechanics and authority boundaries are independently reviewed, reproducible and legally approved.

PHASE 7

FUTURE GATE

Market Bootstrap, Price Authority & SIGNAL Access

Establish sufficient market quality and decentralised price authority before economic-value-based machine locks activate.

- Canonical FLSG/FLR market with protocol-owned liquidity and transparent price discovery.
- Legitimate liquidity, trading history and manipulation-resistance evidence.
- Standard FTSOv2 FLSG/USD price authority established before SIGNAL Access activation.
- Access Epoch 1 gated by freshness, liquidity and price-authority evidence.
- Enhanced, Professional and Institutional immutable lock contracts under published schedules.

VALIDATION GATE FLSG pricing is sufficiently robust and independently sourced for deterministic economic-value lock requirements.

DETAILED ROADMAP

8. Utility-linked burn and cryptographic evolution

PHASE 8

FUTURE GATE

Usage-Derived Burn Activation

Activate revenue-funded FLSG destruction only after real paid usage and market liquidity prove the execution economics.

- Customer product pricing remains independent of the usage-burn mechanism.
- Approved qualifying revenue share enters a one-way burn reserve with no treasury return path.
- Manipulation-resistant acquisition/burn execution with bounded market impact.
- Public access-burn versus usage-burn accounting and execution evidence.
- Prospective economic reassessment without altering active locks or previously committed customer rights.

VALIDATION GATE Measured machine revenue, legitimate liquidity and legal review justify activating the second burn engine.

PHASE 9

FUTURE GATE

Cryptographic & Protocol Evolution

Adopt stronger Flare-native and cryptographic capabilities through explicit new versions without rewriting monetary history or active customer rights.

- Flare Confidential Compute when production-mature and materially trust-reducing.
- Protocol Managed Wallet/native-account capabilities when their security model is production-ready.
- Optional post-quantum protected high-value custody and recovery using standardised cryptography.
- Future native Flare post-quantum/security primitives when mature and audited.
- New immutable contract versions rather than upgrades to live customer-money contracts.

VALIDATION GATE New capabilities preserve existing supply history, lock terms, beneficiaries and customer-property invariants.

CONTROL FRAMEWORK

9. Non-negotiable gates before Mainnet

These gates prevent schedule pressure, hype or funding constraints from weakening the architecture.

GATE	REQUIRED EVIDENCE	WHAT IT PREVENTS
Product	Production intelligence/truth architecture complete.	Token implementation distracting from unfinished product.
Commerce	Real paid machine intelligence proven end-to-end.	Utility resting on theory rather than measured usage.
Specification	V1 contract behavior frozen; evidence-driven configuration resolved.	Coding against moving implementation requirements.
Security	Public invariants plus fuzzing, mutation, AI red-team, formal verification and reproducible builds.	Critical properties relying on one testing method or hidden architecture.
Funding	External/non-destructive funding covers specialist work.	Cheap private sale or founder liquidation to fund audits.
Audit	Independent security audit remediated.	Mainnet customer-money contracts before review.
Legal	UK token/distribution/burn/liquidity structure reviewed.	Public distribution before specialist sign-off.
Liquidity	Sufficient legitimate quote-side liquidity.	Forced launch into a manipulable thin market.
Price authority	Robust FLSG reference pricing, preferably standard FTSOv2.	SIGNAL Access based on a weak invented oracle.
Access	Existing locks immutable; principal inaccessible to admins.	Customer-property rights depending on operator discretion.

WHAT THE ROADMAP DOES NOT PROMISE

- A token-launch date or target return.
- A CEX-listing timetable.
- A guaranteed grant.
- A shortcut around audit or legal review.
- Activation of FCC, PMW or post-quantum features before maturity.

MAINNET READINESS DEFINITION

FLSG reaches Mainnet only when it is the natural next layer of a completed FlareSignal product: real machine demand, proven payments, implementation-ready minimal contracts, non-custodial customer principal, robust Flare-native pricing/trust infrastructure and public on-chain transparency. Security architecture and invariants can be public; credentials, signer locations, live alert thresholds, infrastructure topology and incident-response operations remain private.