

THE FORGE

PROTOCOL PUBLICATION / 01

TECHNICAL WHITE PAPER

Forge Protocol White Paper

hpFLR liquid staking, FIFO redemption and swap aggregation on Flare

SWAP AGGREGATION | ZERO ROUTING SURCHARGE | LIQUID STAKING | CORE OPERATIONS | RELEASE BOUNDARIES

PRODUCTION EDITION - 15 NOVEMBER 2026 UTC

Architecture, implementation boundaries, security model, and deployment evidence.

BUILT FOR FLARE

FORGE PROTOCOL / TECHNICAL PAPER

Document status

This paper describes the active Flare production architecture and its intended initial activation. The first operating phase provides hpFLR minting, delegated staking services, separate holder rewards and FIFO redemption. When eligible FLR backing is generous, a later phase may fund the protocol's own validator self-bond in an amount chosen at that time while maintaining ample rolling delegation stake and FIFO liquidity. The hpFLR contracts, reward services, staking controls, swap aggregator and application are installed; the global operational switch remains paused. The initial hpFLR/WFLR Forge pool and expanded staking-provider configuration are launch preparations, with no pool creation or native staking transaction claimed by this publication. The separate Security Assessment records the review scope, evidence and verdict.

STATUS / SCOPE / AUTHORITY

FORGE / 01

1. Product and economic model

Forge combines hpFLR liquid staking with a swap aggregator for Flare. A deposit of 1 FLR mints 1 hpFLR. The principal conversion remains 1:1 through redemption, while validator and mirrored-stake rewards are separate amounts owed to eligible historical holders. hpFLR does not rebase and its principal exchange rate does not increase when rewards arrive. The protocol charges no deposit, redemption, staking or reward fee.

A holder may keep hpFLR, transfer it, use an admitted liquidity position, or request redemption. Native FLR staked on the P-chain cannot be redeemed immediately from that chain. The FIFO queue and liquid reserve determine when a request is funded; available returned principal pays earlier requests before new staking. The optional delivery services provide transaction liveness under the owner's consent, while contract accounting determines entitlements.

The aggregator searches supported Flare liquidity for an executable route with the best estimated net result. External pools keep their own fees. Forge adds no routing surcharge or protocol swap fee. The planned Forge hpFLR/WFLR pool, when deployed, will charge only its disclosed pool fee, entirely for its LP holders.

FORGE / 02

2. Principal accounting and solvency

The Vault is the only hpFLR minting path. It mints the number of hpFLR units corresponding to FLR actually received. The Vault and bound redemption queue may burn only within their respective accounting paths. Block-number checkpoints preserve historical balances for reward calculations.

The Vault separates liquid principal, pending and confirmed native stake, recorded impairment, funded FIFO allocations, and recognized reward liabilities. It requires its recognized assets to cover modeled liabilities before safety-sensitive actions. `stakeableReserve()` excludes both recognized rewards and every unfunded FIFO exit. A staking release is limited to that reserve and the fixed custody destination. No arbitrary transaction-size cap or artificial refill delay reduces a holder's available liquidity.

An external stake is recorded as an exact on-chain lot with its provider, amount, kind, start, end and lifecycle state. The canonical P-chain stake mirror confirms native exposure. An exact return restores liquid reserve, and mirror lag remains discounted until observed state catches up. A loss is recorded as impairment and can trigger the divergence safeguards. An optimistic mirror reading cannot simply be treated as liquid FLR.

FORGE / 03

3. FIFO redemption

A holder requests redemption by escrowing hpFLR in the queue. Requests have a permanent order; later requests cannot jump ahead by cancellation or re-entry. Available FLR funds positions in that order. A position may be partly funded, with its unpaid amount still outstanding. Once funded, the holder claims the allocated FLR and the corresponding escrowed hpFLR is burned.

Gross principal settlement is 1 FLR per hpFLR. Time to funding depends on actual liquid reserve, native maturity and return, prior queue demand, and network operation. A 14-day delegation term is not a promise of 14-day redemption. Pausing new deposits or reward recognition does not disable already funded native claims.

An owner can opt into automatic funded-claim delivery. The delivery router requires both queue admission and an owner authorization that fixes executor, expiry, gas bounds and minimum net proceeds. A successful delivery reimburses the exact authorized transaction gas from the gross payout; manual claim pays the funded gross amount and the wallet pays its gas separately. This gas reimbursement does not change the 1:1 principal obligation or create a protocol fee. Failed or revoked automation leaves the underlying funded claim available.

FORGE / 04

4. Automated native staking and lot rollover

Three independent policy watchers derive proposed actions from confirmed Flare state, Vault reserve, queue demand, native validator terms and capacity, stake mirror, and signer epoch. Two matching approvals authorize one typed action through the operations controller. A non-voting relayer submits approved C-chain actions; native custody signing requires two independently held threshold shares. Neither a single watcher nor the relayer can choose an arbitrary amount, destination, provider or native action.

Initial native staking uses 14-day rolling delegations to approved providers. Delegation lots have no fixed size or weekly start slot beyond real Flare minimums and available capital. Lots may be staggered across days. When a lot matures, its principal returns through the Vault, funds available FIFO exits, and only then may its remainder form another eligible lot. The automation cannot reserve principal ahead of an unfunded exit merely to preserve a rollover schedule.

The later owned-validator phase uses a distinct 60-day self-bond action for a newly registered NodeID. Its amount is intentionally undefined until the decision is made from actual eligible FLR backing and the desired rolling-stake allocation, within Flare and contract limits. The bond is funded from FLR backing accumulated through hpFLR deposits and returned lots, never by staking hpFLR tokens on the P-chain. Recognized rewards and unfunded FIFO exits remain reserved, and substantial principal must remain available for rolling delegations. The current self-bond planner would use available reserve up to its contract target if enabled; it must not be enabled for the new validator until its sizing and rolling-capital retention policy matches this plan. The new validator also needs its verified node and BLS registration, governed approval, eligible native term, and exact custody and reward-owner bindings. A self-bond cannot be treated as a delegation rollover. If the first custody wallet is assigned to three distinct providers, the new validator also needs a separately provisioned custody wallet and corresponding controller bindings.

The initial provider candidates are 4DadsFTSO (`NodeID-CoNH4gyEwB9gTrEmozwh14Zr8hs6wokRS`), Flare Forward (`NodeID-5amxeiA5AKHPPy6v1C7S1YgmkoXQDedtE`), and Catenalytica (`NodeID-JacLSXQupkEWp14ewzzer6KHxDFksxb8m`). The editable source allowlist stages these three NodeIDs. It does not install them on the production hosts or authorize a native transaction. Current identity, term and capacity must be checked before each actual lot. The governed validator policy must register a node, and the installed watcher, relayer and custody configurations must agree. Flare's staking guidance limits mirrored reward eligibility to the first three distinct validators for one P-chain address; multiple lots with one provider do not use an additional provider slot. A fourth provider would require a separately provisioned custody wallet and matching policy bindings.

FORGE / 05

5. Rewards and holder allocation

P-chain validator rewards and MIRROR rewards are separate streams. The system recognizes only actual received value from the applicable Flare reward managers. Validator rewards enter the Vault as a measured native balance increase and remain separate from hpFLR principal. A scheduled epoch boundary without a funded receipt creates no holder payment.

For each funded period, the calculator uses the owner's private full-history Flare node and a committed future secure random round to choose three distinct historical blocks from the eligible interval. It reads each holder's hpFLR balance at those blocks and attributes balances held inside governed eligible positions to their economic owners. Structural protocol addresses are excluded from eligible supply. The holder's weight is the median of the three effective balances. Each allocation is the funded amount multiplied by that weight divided by total eligible weight, rounded down. Integer dust remains unallocated for later treatment.

The complete artifact commits source block and hash, randomness, snapshot blocks, eligible supply, exclusions, every holder amount, root and proof. A root quorum posts an allocation bounded by actual funded rewards. A challenge interval precedes claims. The cumulative holder ledger credits each accepted allocation once, so a holder sees one outstanding balance rather than a list of small per-epoch claims. A holder may claim that balance as FLR or use an authorized reward-to-hpFLR delivery path. Root correctness still depends on independent reproduction of the published historical calculation; an on-chain Merkle proof checks membership in the posted root, not whether the operator chose fair source data.

Optional personal reward delivery requires the owner's explicit authorization and is limited to fresh rewards, selected asset, expiry, gas bounds and minimum net amount. Manual claims remain available. Gas reimbursement for successful authorized delivery is measured separately from reward entitlement; the protocol takes no service markup.

FORGE / 06

6. Swap aggregation

The live Flare aggregator indexes pools from authenticated factory events across supported venues, including BlazeSwap V2, Enosys V2/V3 and SparkDEX V2/V3/V3.1/V4. The backend uses the owner's private full-history node. Its catalog checks completeness and canonical block identity; stale or incomplete discovery fails closed. Pool discovery is not token endorsement.

Quotes compare direct, multi-hop and atomic split routes. They account for pool output after fees and token deductions, price impact, estimated execution gas and required approval gas where a sound comparison is available. The service presents the best executable result found within its bounded search, not a guarantee of the global optimum or of a future block's price. A quote binds pool, route, chain and block identity. Supported FLR and mapped USD-token routes use a fresh FTSO reference in preflight. The connected wallet rechecks account, chain, balances, allowance, contract identity and simulation before signing.

The Flare swap executor authenticates each pool against its fixed factory, enforces token continuity and user minimum output, and permits neither arbitrary target calls nor arbitrary callback payers. A split's inputs sum exactly to the signed input and its branches settle atomically. External venues retain their own pool fees. Forge adds zero fee to a route that only traverses external pools.

FORGE / 07

7. Planned hpFLR/WFLR Forge pool

The first planned Forge liquidity transaction deposits **1 hpFLR and 1 WFLR**, establishing an opening reserve ratio of one unit of each. This amount is a small initial pool and can produce severe price impact. The pool ratio is a market starting point, not a guaranteed trading price or a change to the Vault's 1:1 principal redemption obligation. A later swap price moves with reserves and trades.

The pool requires minted hpFLR, WFLR, verified Flare factory and router bindings, and a completed creation and liquidity transaction. None of those pool transactions is represented as already done. Once live, the aggregator compares its simulated net output with other supported venues and uses the Forge pool only if its route is competitive for the request. The pool's swap fee belongs entirely to its LP holders; no treasury, referral or governance-token share is taken.

FORGE / 08

8. Operations, control and activation

The active contracts use individually administered upgradeable proxies where applicable. The interim direct administrator and the timelock retain the powers recorded on chain. The direct administrator can permanently forfeit its upgrade ability; it has not done so in the reviewed standby. A 60-second timelock is an administrative delay, not independent governance. The global operational switch gates new activity and remains paused. Recovery and already funded claims retain their separately defined paths.

Signing keys and full-history RPC access stay on private service hosts, outside Pages and browser bundles. The three custody shares are held independently; no complete native custody key runs on the observer. Exact-intent journals reconcile ambiguous C-chain and P-chain submissions before retry. Health services watch required roles, timers and advancing checkpoints. Gas funding supplies operational working capital without changing holder entitlements.

At launch the operators verify current contract identities and provider terms, install the same approved-provider list on the relevant roles, register eligible NodeIDs through governed policy, deliberately activate the switch and staking workers, and verify each resulting mint, delegation, reward and redemption transition. The first hpFLR/WFLR pool transaction is a separate action after the Flare AMM bindings and initial tokens are ready. A new owned validator is introduced later only when its chosen bond size leaves ample capital in rolling delegations after FIFO and reward obligations are reserved, and when node registration and custody capacity are ready. It does not delay the initial minting, delegation, reward and FIFO services. The separate security assessment covers the currently running production standby; future transactions are recorded when they occur.

FORGE / 09

9. Risks and boundaries

Native staking depends on Flare's P-chain, validator availability, reward eligibility and timely principal return. FIFO redemption preserves order and the 1:1 gross obligation but cannot promise instant liquidity. Loss, delayed return or incorrect mirror data can affect backing; accounting and pause controls detect or constrain these conditions without making them impossible.

Historical reward roots depend on complete archived state, correct attribution and honest publication. The challenge interval and public artifact enable independent verification, but a posted root can be wrong if that review fails. Administrators, threshold signers, service hosts, RPC and external venues remain material trust dependencies. Upgrades can repair defects and can also change behavior under authorized control.

A 1:1 opening hpFLR/WFLR deposit does not guarantee a stable pool price. Tiny initial reserves produce large slippage and may make the pool unattractive for ordinary trade sizes. Quotes, network gas, validator returns, reward rates and provider capacity can change. No yield, price or redemption date is guaranteed.

FORGE PROTOCOL / TECHNICAL PAPER

References

- Forge Protocol Security Assessment
- Flare staking and validator limits
- Flare validator tracker
- Flare provider registry



Forge Protocol

Zero-surcharge swap aggregation, liquid staking, and separate rewards on Flare.

Production edition - 15 November 2026 UTC