

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 - 21 NOVEMBER 2026 UTC

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

BUILT FOR FLARE

FORGE PROTOCOL / TECHNICAL PAPER

Document status

This paper describes the current Flare mainnet architecture and its initial launch configuration. 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 for launch standby. The global operational switch remains paused pending deliberate activation. The hpFLR/WFLR Forge pool is live with liquidity and a direct Swap interface; native staking remains on standby. The separate Security Assessment records the assessed production scope, verification and findings.

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 compares supported external Flare liquidity with the live Forge hpFLR/WFLR pool 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 live Forge hpFLR/WFLR stable pool charges **0.30% per swap**. Its entire swap fee accrues to LP tokens; there is no protocol, treasury, referral, governance-token or staking deduction. LP tokens deposited in the Forge LP vault earn their corresponding share, which the vault harvests and makes claimable to vault shareholders.

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

Independent policy watchers derive proposed actions from confirmed Flare state, Vault reserve, queue demand, native validator terms and capacity, stake mirror, and signer epoch. Matching threshold approvals authorize a typed action through the operations controller. A non-voting relayer submits approved C-chain actions. Native custody signers retain separate encrypted key shares and exchange signing messages to produce a transaction signature without reconstructing the private key. Neither an individual 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 approved initial providers are 4DadsFTSO (`NodeID-CoNH4gyEwB9gTrEmozwh14Zr8hs6wokRS`), Flare Forward (`NodeID-5amxeiA5AKHPPy6v1C7S1YgmkoXQDedtE`), and Catenalytica (`NodeID-Lj9wReAAhUQokvp2up5RokYYxkTTPqZRC`). The editable source allowlist and installed custody, relayer and watcher policies agree on these three NodeIDs. Approval does not send a native staking transaction. Current identity, term and capacity must be checked before each actual lot, and the governed validator policy must register the node. 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 live hpFLR/WFLR pair and its LP vault are registered positions in both holder reward streams. At each selected block, hpFLR held by the pair follows ownership of its LP tokens; LP tokens deposited in the vault follow ownership of vault shares. The pair and vault are excluded as direct reward recipients, so their holders receive the attributed share through their wallet balances instead of a claim stranded at a custody contract. This holder allocation is separate from pool swap fees and the vault's WFLR delegation reward stream.

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 external pools from authenticated factory events across supported venues, including BlazeSwap V2, Enosys V2/V3 and SparkDEX V2/V3/V3.1/V4. It also includes the configured, factory-verified Forge hpFLR/WFLR pair. The backend uses the owner's private full-history node. Its catalog checks completeness and canonical block identity; stale or incomplete external discovery fails closed. Pool discovery is not token endorsement.

Quotes compare direct, multi-hop and atomic split routes across supported external pools, and the direct Forge hpFLR/WFLR pair. The Forge pair is not used in mixed or split routes. Quotes account for pool output after fees and token deductions, price impact where measurable, 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. The connected wallet checks fresh FLR/USD, USDT/USD and USDC/USD FTSO feeds for any WFLR, USDt0 or USDC.e asset in the selected route, even when the other token has no configured feed. When both swap endpoints have feeds, their cross-rate also constrains the transaction minimum; a one-sided feed check does not independently price the other token. The Forge hpFLR/WFLR pair separately enforces its own on-chain FTSO guard. The connected wallet rechecks account, chain, balances, allowance, contract identity and simulation before signing.

The Flare swap executor authenticates external pools against their fixed factories, 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. The direct Forge pair uses the Forge router with factory and pair identity checked before signing. External venues retain their own pool fees. Forge adds zero fee to a route that only traverses external pools.

FORGE / 07

7. Live hpFLR/WFLR Forge pool

The hpFLR/WFLR pool was initialized at a 1:1 reserve ratio with deliberately modest liquidity, leaving room for other liquidity providers to add depth. 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. Swap prices move with reserves and trades.

The Flare factory registers the hpFLR/WFLR stable pair, and the Swap page presents it as the primary market. The aggregator can quote and execute this direct pair through the Forge router alongside its search of external venues. Its live pair-specific fee is **30 basis points (0.30%)**. The pair allocates the fee pro rata to LP tokens. The Forge LP vault holds the initial LP position and distributes the fee claims attributable to that position to its vault shareholders. Other holders of this pair's LP tokens receive their own pro rata claims directly from the pair.

Both holder reward registries also recognize the pair and the LP vault. The pair's hpFLR exposure is attributed to LP owners, including owners of shares in the LP vault, for funded MIRROR and validator-lot reward allocations. Each recipient's published allocation enters the cumulative holder reward balance and can be claimed through the normal wallet flow.

Forge pairs support two reserve-pricing curves: the stable curve is designed for assets expected to trade near parity, while the volatile curve follows a constant-product formula for assets with a freely moving relative price. The live hpFLR/WFLR market uses the stable curve. These are pool configurations, not a choice the trader must make in the Swap form. Neither curve guarantees a peg or sufficient liquidity.

The live pair's FTSO policy maps hpFLR and WFLR to the FLR/USD feed, requires a feed no older than **300 seconds**, and rejects a swap whose output exceeds the feed-implied input value by more than **100 basis points (1%)**. The check runs in the pair contract at execution; an invalid or stale feed makes a guarded swap fail. This is an output ceiling, not a two-sided oracle price band. The trader's signed minimum output supplies the lower execution bound relative to the displayed quote. The pair's reserve curve, the FTSO ceiling and the user's minimum output address different risks; none guarantees that hpFLR will trade at 1 WFLR.

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. MANA is the planned governance token and has not been created or distributed as part of the initial operating suite; it is not a staking or liquidity reward token. The global operational switch gates new activity and remains paused. Recovery and already funded claims retain their separately defined paths.

The public Flare interface currently enables hpFLR minting, redemption and reward views subject to the operational switch; Swap compares the configured Forge pair and supported external venues; Liquidity exposes the live hpFLR/WFLR pool; Vaults exposes its LP vault; Wallet & Staking provides native wallet operations. Earn, LaunchPad, Pool Management, MANA staking and public governance are withheld. The operational staking, reward, redemption, quote and safety services described in this paper are the current production modules.

Signing keys and full-history RPC access stay on private service hosts, outside Pages and browser bundles. Custody key 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, provider terms and the matching installed provider policies, register eligible NodeIDs through governed policy, deliberately activate the switch and staking workers, and verify each resulting mint, delegation, reward and redemption transition. The hpFLR/WFLR pool already exists and operates independently of native-staking activation. 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.

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.

An initial 1:1 hpFLR/WFLR reserve ratio and the pair's FTSO output ceiling do not guarantee a stable pool price. The guard does not impose an independent oracle price floor or supply liquidity. Small reserves can produce large slippage and may make the pool unattractive for ordinary trade sizes. USD-token FTSO feeds reflect reported market prices, including a possible depeg; they do not verify an issuer's reserves or bridge solvency. 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 - 21 November 2026 UTC