Quote.Trade

V6 Primary Funding Contracts and V1 Fallback/Hotwallet Architecture

Public-Scope Smart Contract Security Review and Audit Report

Audit Result	Severity Summary	Review Date
PASS	**No Critical / High / Medium findings**	**2026-08-20**

Scope class	**Public smart-contract source/ABI, deployed-address posture, architecture, authorization, accounting, membership, withdrawal, rate-limit, emergency, and read-only companion review.**
In-scope V6 deployment	FundingContractV6 core at 0xfb41c4f731a064fb3911d16d529be0c2958d5fc6 on Ethereum and XDC; FundingContractV6Views at 0x228d706e0651038dd8ec151e2f639b3e47ffecb6 on Ethereum and XDC.
In-scope V1 fallback	Ethereum TransparentUpgradeableProxy at 0x8815e8F0eb65E1072518e8F842C3aD5199DFCEF1, retained only as constrained fallback/hotwallet context.
In-scope position layer	Polygon and XDC PositionManager at 0xf857aC7bed76B43c5457f56483803C4CebbD7eff, retained as positions-only context.
Primary conclusion	V6 receives a public-scope PASS. No Critical, High, or Medium smart-contract vulnerability was identified. Seven non-blocking Low observations and ten Informational or assurance items are documented.

Important limitation
This report assesses the deployed V6 address posture and publicly available Solidity source. It is not a private-engine audit, infrastructure penetration test, signer-custody assessment, formal proof, proof-of-reserves review, legal opinion, or independent deterministic bytecode rebuild. Dynamic chain state can change after the review date. Exact grouped-withdrawal and membership-transition accounting remains outside the public-source scope.

1. Executive Summary

The reviewed production design is a hybrid funding and risk-control architecture. FundingContractV6 is a direct, non-upgradeable custody and settlement core deployed at 0xfb41c4f731a064fb3911d16d529be0c2958d5fc6 on Ethereum and XDC. It stores per-user withdrawable balances by composite. A composite may be Segregated, with one real token, or Grouped-Par, with two or more approved par-value tokens sharing one published balance and one composite-level withdrawal cap. The publisher/offline engine remains responsible for deposit recognition, positions, PnL, signed token-level netting, and exact withdrawal approval before state is published or withdrawals are submitted.

The V6 core preserves the principal V5 containment controls and adds composite accounting: three event-based qualifying slots at least 22 hours apart, a 1.5x minimum-slot cap, a 10-minute post-publication cooldown, duplicate-withdrawal prevention, physical-liquidity checks, conditional per-token hourly and daily limits, emergency freeze and signer rotation, checks-effects-interactions, nonReentrant protection, and exact token/native transfer invariants. Grouped-Par withdrawals consume one shared composite allowance even when the user selects different member tokens.

A separate FundingContractV6Views companion is deployed at 0x228d706e0651038dd8ec151e2f639b3e47ffecb6 on both networks. It holds no funds, exposes read-only reporting and export functions, and cannot mutate or authorize withdrawals. The core does not use the companion as an authorization dependency. This one-way split preserves the core security boundary while providing EIP-170 bytecode headroom.

Production policy sets the stablecoin low-liquidity relief threshold at 1,000,000,000,000 engine units ($1,000,000 for six-decimal stablecoins) per token. Below that physical token balance, the 3% hourly and 18% daily aggregate rate-limit checks are bypassed; the shared user cap, three-slot eligibility, cooldown, registered-wallet restriction, replay protection, liquidity check, emergency controls, and transfer invariants continue to apply. Membership transitions remain seven-day timelocked and are conditioned on complete engine-side conservation and post-change reconciliation before withdrawals reopen.

Executive opinion
PASS - public smart-contract source/ABI and deployed-address scope. No Critical, High, or Medium smart-contract vulnerability was identified. V6 is suitable as the primary funding architecture under the documented hybrid model. Exact private-engine reconciliation, privileged-role controls, deployed configuration, and the constrained V1 fallback remain outside or conditional to this public review.

Severity	Count	Status	Comment
Critical	0	PASS	No Critical public smart-contract issue identified.
High	0	PASS	No High public smart-contract issue identified.
Medium	0	PASS	No Medium public smart-contract issue identified under the documented hybrid architecture.
Low	7	NON-BLOCKING	Seven hardening and operational-integrity observations; none establishes a confirmed unprivileged drain path.
Informational	10	ACCEPTED / REQUIRED CONTROLS	Ten items document publisher/engine dependencies, threshold and availability policy, and build/deployment assurance.

Key conclusion	Assessment
V6 production architecture	Appropriate primary architecture based on reviewed source, direct non-upgradeable posture, deployed addresses, shared composite accounting, and expanded controls.
Grouped-Par accounting	One composite-level 1.5x cap is shared across member tokens. Exact token-level netting and transition allocation remain private-engine dependencies.
Core/views split	Sound. The core is authoritative; the views companion is immutable, read-only, non-custodial, and outside the authorization path.
V6 non-upgradeability posture	Direct constructor-based source and no upgrade ABI surface. New code requires migration rather than an in-place proxy upgrade.
V1 fallback/hotwallet	Acceptable only as a capped, monitored, exception-only path for small, recent deposit-withdraw cases.
Publisher/offline engine	Security-critical hybrid dependency. Exact balance, risk, token-level netting, and membership-transition accounting are outside the public smart-contract scope.

2. Scope, Methodology, and Review Boundaries

Scope includes the deployed V6 core and views contracts, the publicly available V6 Solidity source and ABI, Ethereum and XDC explorer evidence, and the documented hybrid architecture. The assessment covers public source/ABI behavior and deployment posture. It does not certify the private engine implementation, signer custody, solvency, or deterministic reproduction of deployed runtime bytecode from Standard JSON compiler inputs.

In-scope item	Networks / status	Audit purpose
FundingContractV6	Ethereum and XDC Mainnet deployments	Custody core, composites, roles, publishing, withdrawal, conditional rate limits, emergency, membership timelock, and transfer invariants.
FundingContractV6Views	Ethereum and XDC Mainnet deployments	Read-only reporting companion, core linkage, export consistency, and duplicated balance-resolution logic.
V1 funding contract	Ethereum Mainnet USDC/USDT	Fallback/hotwallet only; proxy posture and operating requirements included as contextual scope.
PositionManager contracts	Polygon and XDC	Positions-only context and freshness requirements included as contextual scope.

In-scope item	Networks / status	Audit purpose
Production operating constraints	V6 primary; V1 exception only; $1m per-token threshold	Architecture, collateral, fallback, Grouped-Par, threshold, and operating-policy assumptions supporting the opinion.

Out-of-scope item	Implication
Private engine source and tests	Outside the public-source scope; exact grouped-withdrawal and membership-transition accounting is treated as a hybrid trust dependency.
Deterministic build reproduction	Exact Standard JSON, dependency lock, compiler settings, and local runtime-bytecode reproduction were not independently executed.
Full independent fuzzing / formal verification	Not performed in this public-scope report.
Signer custody and internal approval procedures	Not assessed. Public role separation and emergency controls are reviewed; private custody and procedures are not.
Dynamic chain state after review date	Roles, balances, thresholds, composites, and transactions may change after the review date.
Legal, compliance, accounting, proof-of-reserves, or solvency	Not covered. Token balances and holder pages are point-in-time context only.

Methodology

1. Assess every externally callable function, modifier, role, immutable, storage structure, event, and custom error in the V6 core and views companion.
2. Trace publishing, slot advancement, cap formation, cap consumption, rate-limit, emergency, membership mutation, and transfer flows for fail-open and fail-closed behavior.
3. Evaluate Segregated and Grouped-Par accounting, including cross-token withdrawals against one shared composite cap.
4. Review the explorer-published V6 source and deployed architecture against V5, including composite accounting, the views split, write-once token thresholds, membership timelocks, and publisher-side transition conservation.
5. Map source-level controls to risk classes and document formal findings using severity, status, affected components, evidence, impact, recommendation, and residual risk.
6. Assess V1 fallback and PositionManager operating requirements as contextual components; their code is outside the V6 source-review scope.

Documented production operating constraints
Ethereum uses one Grouped-Par USDC+USDT composite with trading profit netted into one published balance at 1:1 par. XDC USDC remains Segregated. The contract contains no price or exchange-rate oracle logic. For six-decimal production stablecoins, 3% hourly and 18% daily token limits activate at or above 1,000,000,000,000 engine units ($1,000,000 for six-decimal stablecoins); below that level the aggregate rate checks are bypassed, while all user, replay, liquidity, emergency, cooldown, and transfer gates remain. V1 remains a capped fallback for small, recent deposit-withdraw edge cases only.

3. Contract Inventory and Deployment Posture

The inventory separates the deployed V6 custody core, its non-authoritative views companion, the existing V1 fallback/hotwallet, and positions-only ledger surfaces. The V6 core uses the same deterministic address on Ethereum and XDC (0xfb41c4f731a064fb3911d16d529be0c2958d5fc6); the views companion likewise uses the same address on both chains (0x228d706e0651038dd8ec151e2f639b3e47ffecb6).

ID	Component	Network	Address	Evidence posture	Architecture role
F-V6-CORE-ETH	V6 funding core	Ethereum	0xfb41c4f731a064fb3911d16d529be0c2958d5fc6	Publicly identified direct V6 core; source/ABI assessed; public Etherscan Code/Read surface. No proxy architecture appears in the assessed source.	Primary Grouped-Par Ethereum USDC/USDT custody core.
F-V6-VIEW-ETH	V6 views companion	Ethereum	0x228d706e0651038dd8ec151e2f639b3e47ffecb6	Publicly identified read-only companion; immutable core reference in the assessed source; no custody or mutation.	Reporting/export companion only.
F-V6-CORE-XDC	V6 funding core	XDC	0xfb41c4f731a064fb3911d16d529be0c2958d5fc6	Publicly identified direct V6 core on XDC; source/ABI and XDC explorer/token-route evidence included.	Primary Segregated XDC USDC custody core.

ID	Component	Network	Address	Evidence posture	Architecture role
F-V6-VIEW-XDC	V6 views companion	XDC	0x228d706e0651038dd8ec151e2f639b3e47ffecb6	Publicly identified read-only companion on XDC; no authorization role.	Reporting/export companion only.
F-V1-ETH	V1 fallback	Ethereum	0x8815e8F0eb65E1072518e8F842C3aD5199DFCEF1	TransparentUpgradeableProxy posture; fallback-only treatment.	Fallback/hotwallet only; not primary funding.
P-POL	PositionManager	Polygon	0xf857aC7bed76B43c5457f56483803C4CebbD7eff	Positions-only contextual component.	Position publisher state surface.
P-XDC	PositionManager	XDC	0xf857aC7bed76B43c5457f56483803C4CebbD7eff	Positions-only contextual component.	Position publisher state surface.

4. Hybrid Architecture and Reconciliation Flow

The architecture is intentionally hybrid. FundingContractV6 at 0xfb41c4f731a064fb3911d16d529be0c2958d5fc6 is a containment and settlement layer, not a complete on-chain matching, liquidation, margin, or peg-pricing engine. The publisher/offline engine computes the reconciled composite balance and exact withdrawal eligibility; the core enforces bounded on-chain constraints around that trusted state. FundingContractV6Views at 0x228d706e0651038dd8ec151e2f639b3e47ffecb6 is a read-only companion and does not participate in authorization.

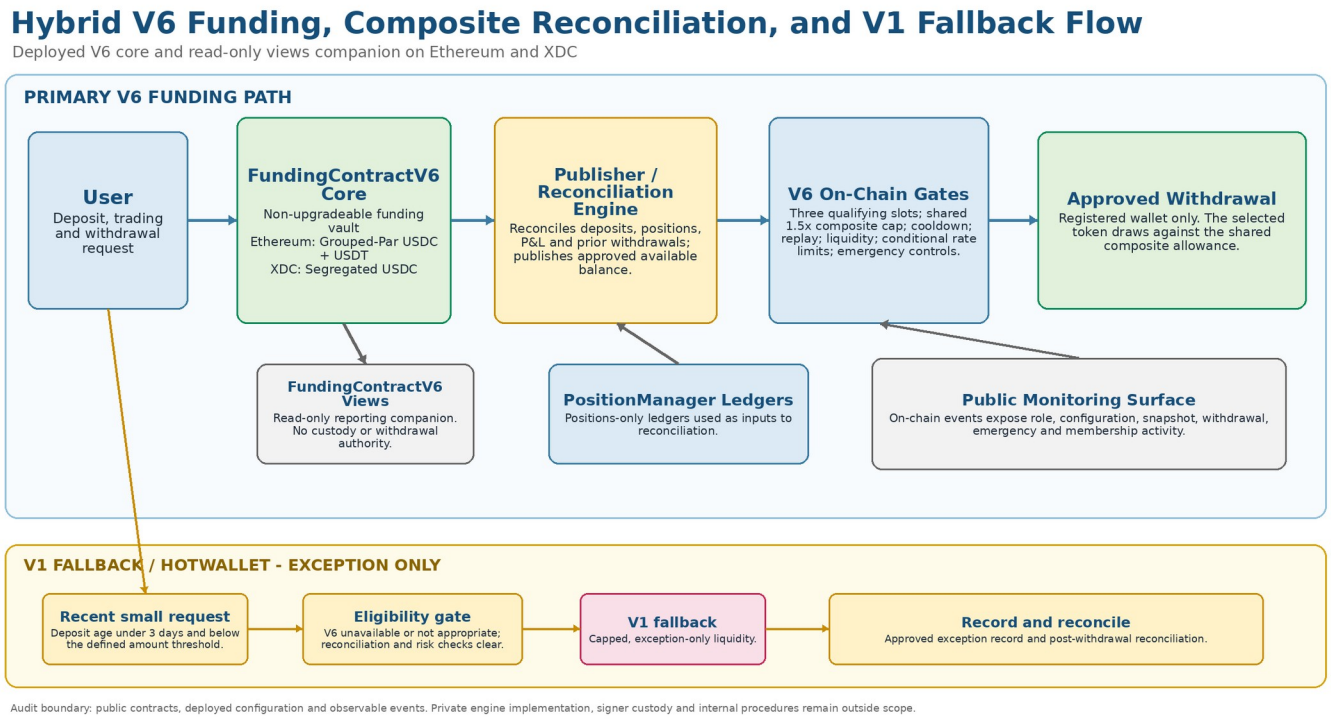

Figure 1. Hybrid V6 primary funding architecture with deployed read-only views companion and V1 fallback exception path.

Required reconciliation and risk checks before V6 withdrawal

Control area	Purpose	Public audit significance
Deposit recognition	Associate on-chain funding with the correct chain, contract, token, and registered user.	Exact private ledger implementation is outside scope.
User, token, and composite mapping	Maintain consistency among wallet registration, token configuration, decimals, and composite membership.	Public configuration and mappings can be inspected on-chain.
Position and composite reconciliation	Incorporate positions, P&L, funding, fees, deposits, and prior withdrawals into exact availability.	The core enforces guardrails around the published result; it does not reproduce this private calculation.
Grouped withdrawal and transition conservation	Apply one composite debit and prevent membership changes from creating excess child availability.	Retained as a required hybrid accounting invariant; private implementation is not assessed.
Snapshot completeness	Prevent incomplete or malformed publication state from being treated as final.	The core provides batch and pending-state guardrails; complete recovery behavior remains a publisher dependency.
Withdrawal eligibility	Combine exact engine approval with on-chain cap, cooldown, replay, liquidity, conditional rate-limit, and emergency checks.	On-chain gates are reviewed; the private approval process is outside scope.
Fallback eligibility	Keep V1 limited to documented, capped exceptions when the normal V6 route is not appropriate.	V1 is contextual scope and must not become the primary funding path.

5. V6 FundingContract Deep Review

FundingContractV6 is a non-upgradeable custodial settlement vault that stores balances by composite rather than by token. A Segregated composite contains one real token. A Grouped-Par composite contains two or more approved six-decimal tokens sharing one published balance and one composite-level cap. The selected token still has its own physical-liquidity and rate-limit constraints. The source retains a three-slot event-based cadence, 1.5x cap, 18% daily and 3% hourly token limits, 10-minute cooldown, three-day emergency freeze, signer rotation, replay protection, and strict transfer invariants. For the production stablecoin routes, those aggregate token limits activate at or above the configured $1 million per-token threshold.

Positive observation	Security value	Evidence / notes
Deployed direct core posture	Reduces routine proxy-admin upgrade risk relative to V1.	V6 core address is separate from V1 proxy; reviewed source has constructor admin and no upgrade ABI.
Core/views one-way split	Keeps custody and authorization in the core while moving reporting-only logic out for code-size headroom.	Views source is immutable/read-only; deployed companion at 0x228d706e...ffecb6.
Grouped-Par shared cap	Prevents the same combined entitlement being drawn independently in USDC and USDT.	executeWithdrawal derives one composite and charges its shared cap sources.
Role-separated operations	Separates admin, guardian, asset manager, balance poster, and withdrawal execution.	Role mappings, signer epochs, and grant/revoke events in the core source.
Timelocked membership controls	Seven-day proposal delay, execution revalidation, provisioning, and a post-change withdrawal latch pending the next completed publication.	Couple, decouple, and merge paths include a seven-day delay, execution revalidation, provisioning state, and a post-change withdrawal latch.
Withdrawal hard gates	Combines engine approval with on-chain cap, cooldown, liquidity, replay, conditional rate, emergency, and transfer checks.	executeWithdrawal and transfer helpers.
Cap-aging hardening	Addresses same-slot inflation, zero basis, aged-source repetition, and carry-forward corner cases.	User-slot update, window aging, minimum-cap, and charge paths.

5.1 V6 funding protections

Protection	How it reduces risk
Approved collateral configuration	Only current-epoch asset-manager accounts can register or re-enable collateral. Decimals and the low-liquidity threshold are write-once.
Segregated and Grouped-Par composites	One-token composites preserve segregated behavior; multi-token composites share one combined balance and cap.
Par-value mechanical restriction	Multi-token creation, couple, and merge paths require six-decimal members. This reduces accidental inclusion of native or non-par decimal assets, though explicit par eligibility remains preferable.
Registered-wallet withdrawal path	executeWithdrawal transfers only to the registered user address and exposes no arbitrary recipient parameter.
Registration-anchored eligibility	Slots committed before user registration do not count toward the user's three-slot cap test.
Three event-based qualifying slots	Withdrawals require a fully populated three-slot composite ring; slots need not occur on consecutive calendar days.
At least 22 hours between qualifying commits	A completed publish advances the ring only when the prior committed slot is at least 22 hours old; delayed publishing does not reset prior slots.
Structured multipart publication	Headers include snapshotId, batchIndex, and totalBatches; strict +1 sequencing applies after the first bounded ID; duplicate indexes and malformed bodies revert.
Pending snapshot withdrawal block	A valid outstanding pending slot blocks withdrawal until completion or an emergency-floor recovery rule clears stale pending state.
10-minute post-publish cooldown	Every committed publish refreshes lastPublishTime and temporarily blocks withdrawals.
Shared lowest-slot 1.5x cap	The user ceiling is the minimum remaining cap across three qualifying composite slots, shared across every token in the composite.
Zero publish hard-close	Publishing zero wipes balance, capBasis, and capConsumed for the slot; a zero basis is treated as authoritative rather than unset.
Replay protection	processedWithdrawals permanently blocks reuse of the same withdrawalId.
Physical token liquidity	The contract checks the actual selected-token/native balance before transfer.
Conditional per-token 3% hourly / 18% daily limits	Rate ledgers are keyed by physical token. For production six-decimal stablecoins, these limits activate at or above the $1 million per-token balance threshold.
$1 million stablecoin relief threshold	Below 1,000,000,000,000 six-decimal engine units, the 3%/18% checks are bypassed for that token. Shared cap, slot, cooldown, replay, liquidity, emergency, and transfer controls still apply.
Exact unit conversion	Withdrawals require exact engine-unit/token-unit round trip, preventing fractional dust or scale mismatch.
Strict transfer invariants	ERC-20 transfers require exact contract debit and recipient credit; native transfers require exact debit.
Reentrancy and CEI	executeWithdrawal is nonReentrant and records replay, rate, cap, and balance effects before external transfer.
Emergency freeze and signer rotation	Admin or guardian can trigger a three-day freeze, invalidate old history, increment signer epoch, and require re-grants.
Native recovery boundary	recoverNative is blocked whenever native currency has been registered as collateral on that chain.

5.2 V6 withdrawal gating sequence

A V6 withdrawal must pass all of the following before funds leave the core contract:

1. The selected token belongs to an existing composite and remains supported.
2. The user address is nonzero, mapped, and registered.
3. Emergency mode is inactive and the withdrawal signer is valid for the current signer epoch.
4. withdrawalId is nonzero and has not been processed before; amount is nonzero.
5. Token amount converts exactly to six-decimal engine units and back without loss.
6. The composite has a latest slot identity and a fully populated, cadence-valid three-slot ring.
7. No valid pending multipart snapshot exists for the composite.
8. The 10-minute cooldown after the latest committed publish has expired.
9. No membership-transition latch remains outstanding for the composite.
10. The user has three valid cap entries tied to slots committed at or after registration.
11. Requested engine amount does not exceed the minimum remaining shared composite cap.
12. The selected token/native pool has sufficient physical liquidity.
13. If the physical token pool is at or above its configured threshold, the 3% hourly and 18% daily token limits are not exceeded; below the production $1 million stablecoin threshold, those two aggregate checks are bypassed.
14. Rate-ledger, replay, cap-consumption, and current-balance effects are recorded before transfer.
15. The transfer succeeds with exact debit/credit or native-debit invariant checks.

5.3 Grouped-Par accounting and membership transitions

Grouped-Par does not create a second allowance for each token. The composite is the on-chain accounting unit. A user may choose a member token for settlement, but every withdrawal consumes the same shared cap. The private engine must debit value against the complete composite and retain any signed token-level debt or cross-token allocation. During couple, decouple, or merge, it must ensure that aggregate child withdrawal capacity never exceeds the parent remaining capacity, that no positive child is published while an offsetting negative component is stranded elsewhere, and that profit is counted exactly once.

Design element	Audit assessment
Shared user balance	Publisher posts one engine-unit balance per user and composite, not one independently withdrawable balance per member token.
Shared cap consumption	Any USDC or USDT withdrawal charges the same composite sources; ordinary cross-token double withdrawal is prevented.
Per-token liquidity	A combined balance does not guarantee that every member pool can satisfy the full amount; each selected pool is checked separately.
Per-token rate limits	3% hourly and 18% daily counters are independent for each physical token.
No on-chain pricing	The core performs unit conversion only. Peg judgment and signed token-level netting remain in the engine.
Membership timelock	Couple, decouple, and merge wait seven days; target/successor composites may pre-season during that period.
Transition conservation	Before any post-change publication releases withdrawals, the engine must net all signed legs, withdrawals, PnL, fees, and funding; allocate profit once; and prove aggregate child capacity <= parent remaining capacity.

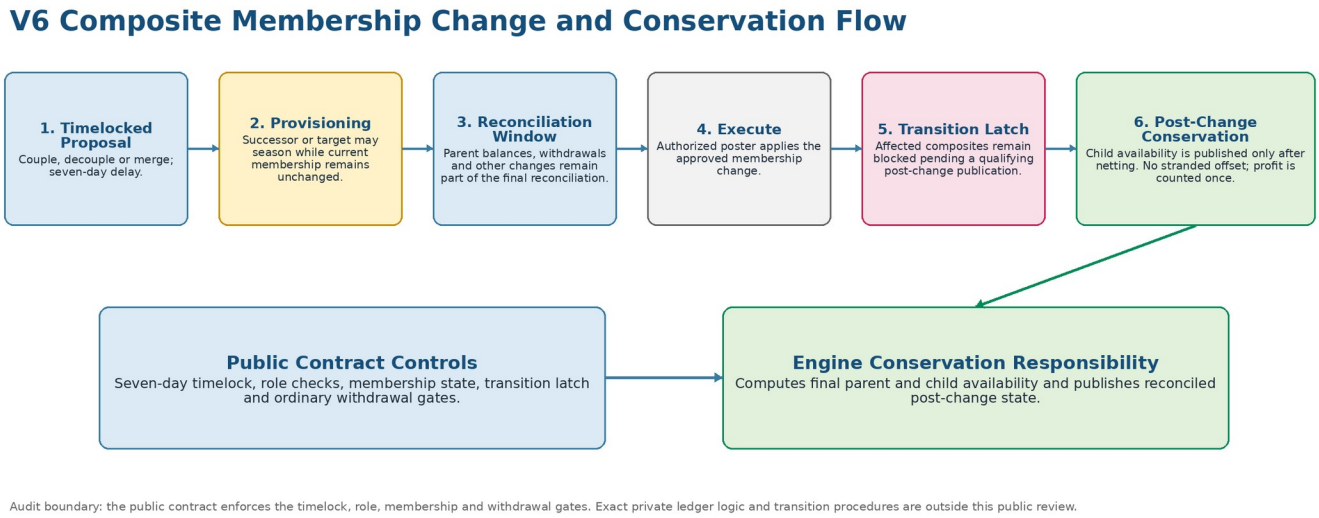

Figure 2. V6 membership mutation, engine conservation, cutover, and required post-change reconciliation.

5.4 Emergency-mode design

Emergency mode is intended for compromise response, especially publisher, withdrawal, or asset-manager key compromise. Activation resets the freeze to three days from the latest trigger, increments signerRotationEpoch, requires balance-poster, withdrawal, and asset-manager accounts to be re-granted for the new epoch, and raises balanceHistoryFloor to the trigger timestamp. Recovery requires three cadence-valid post-floor slots. The freeze and clean-history requirements run concurrently.

The timestamp-floor design has a narrow same-timestamp ambiguity on chains that permit consecutive blocks with equal timestamps. A dedicated emergency epoch attached to each slot would provide stronger exactness than a >= timestamp comparison. This is treated as an informational hardening item rather than a confirmed drain path.

5.5 FundingContractV6Views review

Observation	Assessment
Immutable linkage	The companion stores an immutable core address and has no setter, proxy, or upgrade mechanism.
No custody or mutation	Every external function is view-only; the companion holds no funds and cannot change withdrawal eligibility.
One-way dependency	The companion reads the core; the core does not call the companion for publication, withdrawal, emergency, membership, or authorization.
Export consistency gate	Bulk binary and CSV exports revert while batchesReceived differs from batchesExpected.
Retired-composite handling	getCompositeStatus and current-balance functions now reject nonexistent or retired composites.
Duplicated resolution logic	The companion reimplements the core's _resolveBalance algorithm and can drift if the core changes without a matching update.
Canonical binding check	The public read contract should show the core canonical views address equals the deployed companion and the companion core() points back to the V6 core.

5.6 V6 limitations accepted under the hybrid model

Limitation / dependency	Treatment in audit
Engine and reconciler are security-critical	Accepted. Exact trading, P&L, exposure, peg judgment, token-level netting, and balance truth are off-chain by design.
Balance poster remains high impact	Accepted. A trusted poster can affect published availability; three-slot seasoning, rate limits, role separation, and emergency controls provide containment rather than full trust elimination.
Post-withdrawal reconciliation	Required hybrid dependency. Published availability must reflect prior withdrawals before additional authority is granted.
Sparse publication / omitted unchanged users	Supported only when omitted state is genuinely unchanged; stale changed state is not a valid operating assumption.
$1 million conditional rate relief	Accepted public configuration. Below the configured per-token threshold, aggregate 3%/18% limits do not apply; all other withdrawal gates remain.
Views are reporting guardrails, not authorization	Accepted. The views companion reports state but cannot approve or execute withdrawals.
Incomplete multipart publication recovery	Accepted publisher dependency. The public contract blocks valid pending runs, while full private recovery handling remains outside scope.
Grouped withdrawal and membership-transition conservation	Required engine invariant. Combined child availability must not exceed final parent availability after netting.
Fixed first-withdrawal daily budget	Accepted conservative availability policy. Once active, the daily budget is fixed until the next UTC day.

V6 conclusion
The deployed V6 core and views architecture receives a public-scope PASS under the documented hybrid model. The shared Grouped-Par cap, withdrawal containment, direct non-upgradeable posture, and core/views split are sound. Remaining Low items are non-blocking hardening observations. Exact private-engine reconciliation and privileged-role controls remain residual trust assumptions.

6. Non-Upgradeability and V6 vs. V1 Comparison

The deployed V6 core is represented by the direct FundingContractV6 source and exposes no proxy-upgrade, delegatecall, upgradeTo, or upgradeToAndCall architecture. The read-only views companion is also direct and immutable. The public deployment addresses are 0xfb41c4f731a064fb3911d16d529be0c2958d5fc6 for the core and 0x228d706e0651038dd8ec151e2f639b3e47ffecb6 for the companion on both Ethereum and XDC. This report did not independently reproduce the exact Standard JSON build and runtime bytecode, so local deterministic-build equivalence remains an assurance item. V1 remains an explicit TransparentUpgradeableProxy and retains separate proxy-admin risk.

Risk area	V6 primary posture	V1 fallback posture	Audit treatment
Contract posture	Direct core at 0xfb41c4f7...8d5fc6; read-only views at 0x228d706e...ffecb6.	TransparentUpgradeableProxy at 0x8815e8F0...CEF1.	V6 removes routine proxy-admin risk; deterministic build and migration discipline remain important.
Change model	New code requires controlled redeployment and migration.	Implementation can be changed through proxy governance.	V6 lowers unauthorized upgrade risk but increases migration discipline.
Withdrawal controls	Three-slot shared cap, cooldown, replay, physical liquidity, conditional rate limits, emergency, and transfer invariants.	Earlier implementation and proxy governance determine controls.	Normal withdrawals use V6; V1 only narrow exception path.
Publisher model	Composite balance publication with batch/slot guardrails and engine-side signed token netting.	Not the primary normal-balance publisher.	Publisher correctness remains critical; V6 adds stronger containment.
Incident containment	Guardian emergency, history floor, signer epochs, role revocation, and V6 migration path.	Proxy monitoring and fallback caps required.	V6 is stronger if roles and engine controls are enforced.

7. Role and Permission Matrix

Actor / role	Expected capability	Abuse or failure risk	Public audit consideration
Immutable admin	Grant or revoke roles, close genesis, bind views, and govern membership proposals.	Unsafe configuration or governance action.	High-impact governance role; private custody and approval procedures are outside scope.
Guardian	Activate global emergency.	Improper activation or delayed response.	Emergency authority is visible on-chain; incident procedures are outside scope.
Asset manager	Register or enable assets and create genesis composites before closure.	Incorrect decimals, threshold, collateral, or grouping.	Configuration authority is security-critical and publicly observable through state and events.
Balance poster / publisher role	Register users, publish composite balances, and execute eligible membership changes.	Incorrect balances, incomplete runs, or premature transition release.	Source-level publication guardrails do not replace correct off-chain accounting.
Withdrawal role	Submit withdrawals approved by the hybrid control plane.	Unauthorized execution if private approval or signer controls fail.	Execution remains bounded by the reviewed on-chain gates; the private approval process is outside scope.
Publisher / offline engine	Compute exact reconciled availability and transition allocation.	Incorrect netting can affect published authority.	Central residual trust dependency of the hybrid model; implementation was not audited.
Views companion	Expose read-only balances, snapshots, exports, and status.	Incorrect binding or resolver drift can mislead reporting.	Non-custodial and non-authoritative; correctness depends on parity with core state.
V1 proxy admin	Control the fallback proxy implementation.	Upgrade or admin abuse can affect fallback funds.	V1 remains upgradeable and should remain capped and exception-only.
Monitoring surface	Observe role, snapshot, membership, threshold, withdrawal, emergency, and proxy events.	Missed changes can delay detection.	Ongoing monitoring is outside this point-in-time audit.

8. Security Control Mapping

Risk class	V6 control family	Purpose	Hybrid dependency
Fast deposit-withdraw abuse	Registration-anchored three-slot cadence; 10-minute cooldown; V1 age policy.	Requires multiple qualified observations before normal extraction.	Exact eligibility and reconciliation remain off-chain.

Risk class	V6 control family	Purpose	Hybrid dependency
Grouped cross-token over-withdrawal	Composite-level cap, composite-keyed cap consumption, and exact engine approval.	USDC and USDT share one on-chain containment ceiling.	The engine must apply the complete composite debit; private implementation is outside scope.
Membership partition risk	Seven-day timelock, provisioning, transition latch, and engine conservation.	Provides notice and blocks immediate post-cutover withdrawal.	Final parent/child conservation remains an off-chain accounting dependency.
Replay	processedWithdrawals and unique withdrawalId.	Prevents the same withdrawal from executing twice.	Withdrawal-ID generation and approval workflow are outside scope.
Asset drain / velocity risk	Per-token 3% hourly and 18% daily ledgers above the configured threshold.	Slows aggregate outflow once a token pool reaches the threshold.	Below-threshold outflow remains subject to the other withdrawal gates.
Malformed / duplicate batches	Length, alignment, range, count, deduplication, and sequence checks.	Rejects malformed payloads and duplicate indexes.	Complete private recovery handling remains a publisher dependency.
Membership overlap	Timelock, provisioning target, and source/target transition latch.	Prevents withdrawal before a qualifying post-change publication.	The publication must reflect reconciled state; exact process is outside scope.
Emergency containment	Global emergency, signer epoch, history floor, and clean three-slot recovery.	Freezes withdrawals and invalidates old signer grants and history.	Internal incident procedures are outside scope.
Token behavior anomalies	SafeERC20 and exact transfer invariants.	Rejects fee-on-transfer, rebasing, and unexpected transfer behavior.	Collateral-selection governance is outside scope.
Asset configuration	Asset-manager role, write-once decimals/threshold, and multi-token decimal checks.	Reduces scale and configuration mistakes.	Current public configuration can be inspected; private governance procedures are outside scope.
Read consistency	Immutable views core and SnapshotInProgress export gate.	Reduces reporting inconsistency during multipart publication.	Views/core parity remains a maintenance dependency.

9. V1 Fallback/Hotwallet Review

V1 is not treated as the primary funding architecture. The Ethereum V1 address 0x8815e8F0eb65E1072518e8F842C3aD5199DFCEF1 remains a TransparentUpgradeableProxy and therefore has a different upgrade-governance and hotwallet risk posture from the direct V6 core. V1 should remain a tightly constrained fallback for small, recent deposit-withdraw edge cases only, with numeric caps, independent approval, and continuous monitoring.

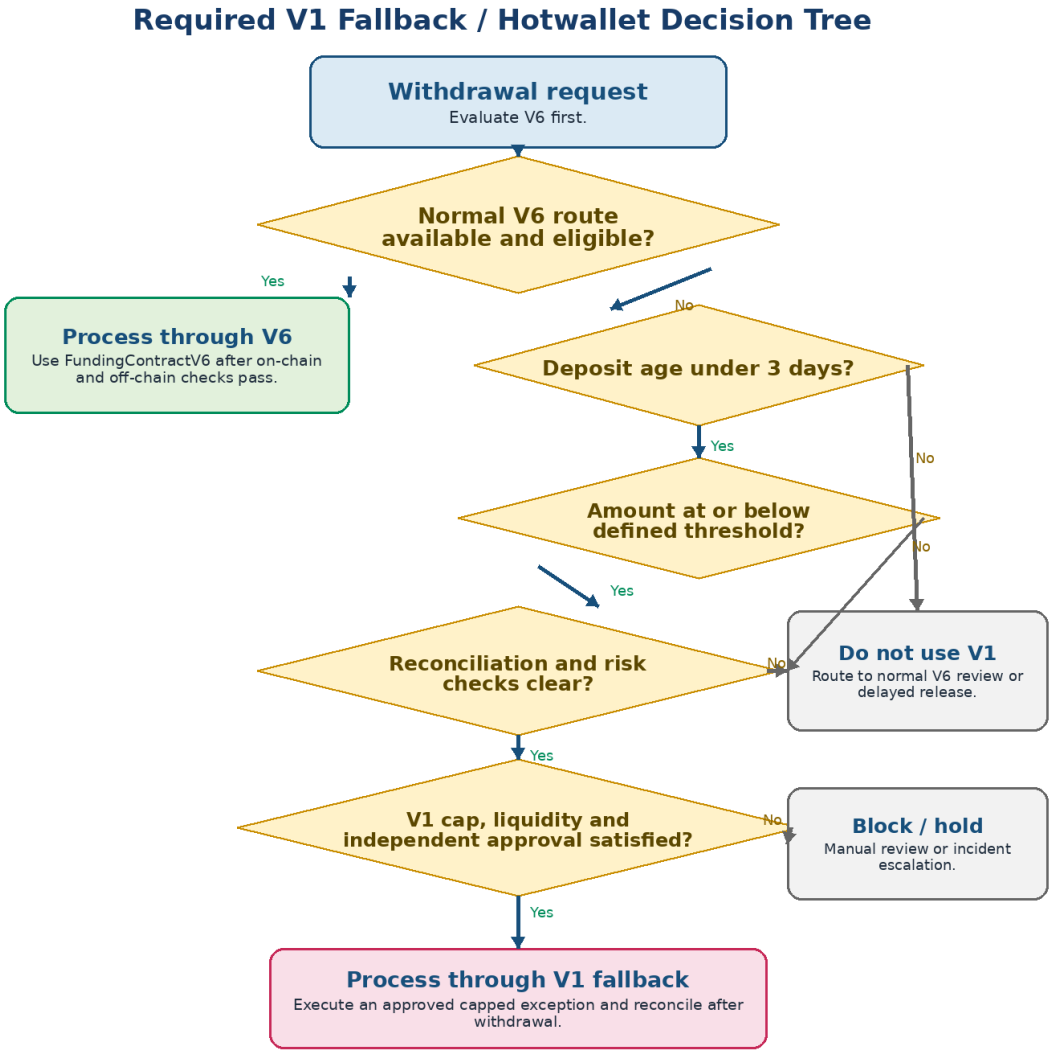

Figure 3. Required V1 fallback/hotwallet decision tree.

Fallback condition	Required interpretation
Deposit age less than 3 days	Maximum eligibility condition for an edge case, not a default withdrawal SLA.
Small amount	Must be numerically defined per asset, user, and rolling window before production reliance.
Clean reconciliation and risk checks	Engine must confirm no suspicious activity, exposure mismatch, unresolved funding risk, or stale balance state.
V6 unavailable or not appropriate	V1 may be considered only when normal V6 processing cannot safely or efficiently handle the request.
V1 balance cap and liquidity	V1 should hold only capped operational liquidity sized to fallback demand, not platform-wide liabilities.
Independent approval and logging	Every fallback withdrawal should have a documented approval and post-withdrawal reconciliation record.

V1 conclusion
V1 remains acceptable only as a tightly capped exception path. It should be excluded from normal primary-funding language and continuously monitored for proxy-admin changes, abnormal outflows, balance-cap violations, and fallback-policy exceptions.

10. PositionManager Review

The Polygon and XDC PositionManager contracts remain in scope as positions-only ledger and withdrawal-request/event surfaces. Their code is outside the V6 source-review scope. V6 reconciliation and withdrawal approval should continue to reject stale or incomplete position state.

Observation	Established posture	Audit significance
Contract identity	PositionManager on Polygon and XDC	Confirms positions-layer role rather than funding custody.
Freshness	lastSyncedTime / syncFrequency style state	Alert and block dependent risk decisions when stale.
Batch completeness	processedBatches / totalBatches / snapshot state	Block dependent decisions until the active batch is complete.
Roles	Updater/admin authority	Monitor every role and mapping change.
Custody posture	Positions-only and non-custodial	Do not market PositionManager as a funding wallet.

11. Deployment Evidence and Transaction Sampling

Source-level analysis is combined with the deployed V6 address inventory and public explorer evidence. Because the deployments are new, public activity and balances are point-in-time evidence rather than a complete transaction audit or solvency attestation. The evidence set includes the Ethereum and XDC core and views addresses, the Ethereum read-contract surface, token-holder/transfer pages for Ethereum USDT and XDC USDC, and the assessed core and views source files. Exact role holders, thresholds, composite membership, genesis closure, views binding, and live balances should be monitored continuously through the read contract and emitted events.

Evidence item	Basis	Audit use	Status
E1 - FundingContractV6.sol	Explorer-published V6 core source	Architecture, roles, composite accounting, publishing, cap/rate logic, emergency, withdrawal, membership, and transfers.	Source-level control coverage completed; deterministic local bytecode rebuild remains an assurance item.
E2 - FundingContractV6Views.sol	Explorer-published V6 views source	Immutable core reference, read-only exports, status, snapshots, and duplicated balance resolution.	Read-only boundary confirmed; no custody or authorization path.
E3-E6 - V6 explorer deployments	Core 0xfb41c4f731a064fb3911d16d529be0c2958d5fc6; views 0x228d706e0651038dd8ec151e2f639b3e47ffecb6 on Ethereum and XDC	Address posture, public source/ABI/read surfaces, chain separation, and deployment inventory.	Included; exact local Standard JSON rebuild not performed.
E7-E9 - Read/token route evidence	Ethereum Read Contract; Ethereum USDT holder/transfers; XDC USDC holder/transfers	Configuration and route monitoring reference points.	Included as public evidence; dynamic point-in-time state.
E10-E12 - Existing public context	V1 fallback and PositionManager public evidence	Fallback and positions-layer posture.	Contextual scope; no new V6 code assessment.
Private engine and complete test suite	Outside the public-source scope	Grouped withdrawal netting, membership conservation, and production integration.	Outside the public smart-contract scope.

12. Formal Findings

No Critical, High, or Medium smart-contract vulnerability was identified within the reviewed public-source and deployed-address scope under the documented hybrid architecture. The detailed Informational findings below define publisher/reconciler invariants, the membership-transition conservation requirement, the conditional $1 million rate-limit threshold, conservative daily-budget behavior, and deployment assurance that must remain controlled for the PASS opinion to hold.

QT6-I07: Incomplete multipart snapshot recovery is a publisher/reconciler invariant

Severity	**Informational / Operational dependency**
Status	Accepted; hybrid publisher dependency
Affected components	FundingContractV6 multipart publication and the private publisher/reconciler
Description	Only the authorized balance poster can submit multipart balance runs. The contract provides batch, sequence, and pending-state controls, while complete crash and recovery behavior remains part of the private publisher control plane.
Impact	Incorrect private recovery handling could cause partial publication state to be treated as authoritative. Ordinary users cannot initiate this condition.
Evidence	Core source includes sequential snapshot IDs, direct row updates, batch-completion state, and withdrawal blocking for valid pending state.
Recommendation	Maintain durable, complete snapshot-state handling and tested recovery so incomplete write-bearing runs are never treated as final.
Residual risk	Operational correctness remains a residual trust assumption of the authorized publisher.

QT6-I08: Membership transitions require complete post-change publisher reconciliation

Severity	Informational / Operational dependency
Status	Accepted; engine conservation required
Affected components	Grouped-Par withdrawal accounting and membership transitions
Description	The core applies one shared cap within a composite, while exact signed token-level balances and profit allocation remain off-chain. Successor and target composites have independent on-chain histories.
Impact	Incorrect private transition accounting could create aggregate child availability above the final parent availability. Ordinary users cannot propose, execute, publish, or approve the transition.
Evidence	V6 source includes provisioning composites, composite-keyed user slots and cap consumption, a seven-day timelock, and a post-change withdrawal latch.
Recommendation	Maintain conservation-safe transition accounting so combined child availability never exceeds final parent availability after all withdrawals, P&L, fees, and funding are netted.
Residual risk	The core cannot independently reconstruct the private signed engine ledger.

QT6-I09: Daily withdrawal budget is intentionally fixed by the first withdrawal of each UTC day

Severity	**Informational / Availability tradeoff**
Status	Accepted by design
Affected components	FundingContractV6 per-token rate-limit policy
Description	Once the per-token limiter is active, the daily budget is fixed from the physical pool observed at that token's first withdrawal of the UTC day. Below the configured $1 million stablecoin threshold, the aggregate hourly and daily checks are bypassed while withdrawals remain recorded.
Impact	A material refill may not increase same-day withdrawal capacity, and sub-threshold outflow is not constrained by the aggregate rate limits. Other user, replay, liquidity, cooldown, emergency, and transfer gates remain.
Evidence	Core source and public configuration expose the fixed daily budget and write-once per-token threshold.
Recommendation	Treat the threshold and daily-budget behavior as disclosed availability and containment policies.
Residual risk	Conservative availability after a refill and a deliberate sub-threshold rate-limit tail; no independent excess-withdrawal path.

Low and hardening findings

QT6-L01: Same-slot multipart corrections remain unsupported

Severity	Low / functional
Status	Accepted constraint or future hardening
Affected components	FundingContractV6 multipart publication
Description	A same-slot correction targets an already committed slot. The first non-final batch reverts, so only single-batch corrections can complete within the 22-hour merge window.
Impact	Large corrections within the 22-hour same-slot window may need to be delivered in one batch or wait for a fresh uncommitted slot. This is an availability and integration constraint, not a custody bypass.
Evidence	E1: non-final commit path rejects a committed publishedSlot.
Recommendation	Document and enforce single-batch same-slot corrections, stage correction overlays, or deliberately wait for the next fresh slot for large reconciliation runs.
Residual risk	Availability and operational complexity; no direct external drain.

QT6-L02: Disabling one grouped token does not freeze the remaining composite

Severity	Low / operational risk
Status	Open hardening
Affected components	Asset configuration and grouped withdrawal path
Description	Disabling one member token blocks withdrawal of that token but does not freeze the composite or invalidate the combined published balance.
Impact	During a depeg, users may continue drawing the stronger member token against a grouped balance that still reflects the weak token. Global emergency is currently the safe response.
Evidence	E1: setSupportedAsset changes only token support; executeWithdrawal checks the selected token, not support status of every composite member.
Recommendation	Immediately freeze the composite or cross-token withdrawals when any member is disabled; allow risk-off decouple of a disabled token; require post-change reconciliation before reopening.
Residual risk	Manageable with a tested global-emergency runbook until hardened.

QT6-L03: Low-liquidity threshold is unbounded and irreversible

Severity	Low / privileged configuration
Status	Accepted configuration discipline; verify production value
Affected components	AssetConfig and setSupportedAsset
Description	The low-liquidity threshold is write-once and not protocol-bounded. Production policy sets 1,000,000,000,000 engine units for each six-decimal stablecoin.
Impact	An incorrect initial value could permanently cause the aggregate limiter to activate too early or too late for that deployment.
Evidence	E1: lowLiquidityThresholdEngineUnits is accepted at first registration and cannot be changed.
Recommendation	Verify the exact AssetConfigured event and tokenConfig read result on each chain; alert on any mismatch; do not accept customer funds until confirmed.
Residual risk	Requires privileged misconfiguration; role custody and deployment review are compensating controls.

QT6-L04: Six decimals are used as the Grouped-Par eligibility test

Severity	Low / governance hardening
Status	Open hardening
Affected components	Composite creation, couple, and merge
Description	Multi-token composites require six-decimal members, but decimals are not proof of economic parity or approved collateral identity.
Impact	An asset-manager error could group an economically non-par six-decimal token and expose stronger collateral to 1:1 redemption pressure.
Evidence	E1: NotParValueAsset checks tokenConfig.decimals == 6 in grouping paths.
Recommendation	Add immutable parEligible configuration or an explicit allowlist and enforce it in every membership-growing path and at execute-time revalidation.
Residual risk	Narrow approved collateral set and asset-manager governance reduce the risk.

QT6-L05: Unknown user IDs are silently skipped and publication totals can overstate applied rows

Severity	Low / reconciliation observability
Status	Open hardening
Affected components	batchSetCompositeBalances and publication events
Description	A record whose userId has no mapping is skipped rather than reverting, while the raw record count contributes to updatedUsers.
Impact	Publisher and monitoring may believe a row was applied when it was not, concealing registry/payload mismatch.
Evidence	E1: parser continues when userMapping[userId] is zero; count is passed to publication progress.
Recommendation	Revert on unknown IDs or count and emit only successfully applied rows.
Residual risk	No direct custody bypass; reconciliation assurance is reduced.

QT6-L06: Canonical views-contract binding lacks validation and a dedicated event

Severity	Low / deployment integrity
Status	Open hardening
Affected components	FundingContractV6 setViewsContract and FundingContractV6Views constructor
Description	The core permanently accepts a configured address without checking code or confirming that the companion core() points back to the funding core.
Impact	A deployment mistake can permanently direct the canonical UI/reconciliation endpoint to the wrong contract, even though core custody remains safe.
Evidence	E1/E2: one-time viewsContract setter; immutable companion core; no backlink validation or dedicated setting event.
Recommendation	Require nonzero code, validate views.core() == address(this), and emit ViewsContractSet.
Residual risk	Core security is unaffected, but reporting and operational tooling can be misdirected.

QT6-L07: Timelocked proposal meaning can drift before execution

Severity	Low / governance intent
Status	Open hardening
Affected components	Membership and merge proposals
Description	Proposals record target/source identities but do not bind complete membership epochs or member hashes. Concurrent changes can alter composite meaning during the seven-day delay. Proposals also have no expiry.
Impact	A transaction may remain technically executable while differing from the state observers understood at queue time.
Evidence	E1: execute-time revalidation checks selected facts but no expected membership epoch/hash or grace period is stored.
Recommendation	Track membershipEpoch, bind expected epochs/member hashes in proposals, and add a bounded execution grace period.
Residual risk	Live-state validation prevents many unsafe executions, but governance notice can become stale.

Informational / assurance items

ID	Item	Public audit note
QT6-I01	Emergency timestamp floor has a narrow same-timestamp edge	A dedicated emergency epoch could provide more exact pre/post-trigger separation in a future version.
QT6-I02	userRegisteredAt source comment is obsolete	The comment should be corrected; the cap-eligibility path does use registration time.
QT6-I03	Views duplicate core balance resolution	Core/views parity must be maintained whenever resolution logic changes.
QT6-I04	Genesis closure is a deployment-state requirement	The irreversible genesis-closed state is publicly verifiable and should precede normal production use.
QT6-I05	Proposal expiry is desirable	A bounded execution period after the timelock would reduce stale-governance intent.
QT6-I06	Independent deterministic build reproduction was not performed	The review relies on public source/ABI and deployed-address posture rather than a separately reproduced Standard JSON build.
QT6-I10	$1 million per-token threshold leaves a deliberate unthrottled tail	Below the configured stablecoin threshold, 3%/18% aggregate checks are bypassed; all other withdrawal gates remain.

13. Security Assumptions and Residual Risks

Assumption	Public audit treatment
Privileged roles are security-critical	V6 separates admin, guardian, asset-manager, balance-poster, and withdrawal functions. Private custody and approval procedures are outside scope.
Publisher/reconciler is authoritative for exact availability	The core enforces guardrails around published balances but does not reproduce the private trading, P&L, exposure, and token-level accounting engine.
Membership transitions depend on post-change conservation	The public contract provides a timelock and transition latch; exact parent/child allocation remains an off-chain dependency.
Emergency and migration readiness	Public emergency, signer-rotation, and non-upgradeability controls are reviewed. Internal incident and migration procedures are not disclosed or assessed.
V1 remains exception-only	V1 is treated only as a capped fallback/hotwallet path and not as a parallel primary funding wallet.

Residual risk	Public audit treatment	Scope note
Offline reconciliation correctness	Hybrid trust assumption; exact private accounting cannot be independently proven from public source.	Private engine outside scope.
Privileged signer compromise	Role separation and emergency controls reduce impact but cannot prove key custody.	Signer custody outside scope.
Publisher fabrication over time	Three-slot seasoning and conditional token-level rate limits contain but do not eliminate trusted-publisher risk.	Operational trust remains.
Membership-transition error	Timelock and transition latch reduce risk; exact conservation remains off-chain.	Private engine outside scope.
Conditional rate-limit tail	Below the configured per-token threshold, aggregate rate limits are bypassed; all other gates remain.	Public configuration disclosed.
V1 fallback misuse	Residual policy risk exists if V1 ceases to remain capped and exceptional.	Contextual fallback scope.
Dynamic monitoring gaps	Ongoing alert coverage and changing chain state are outside this point-in-time review.	Post-review state may change.

14. Final Opinion

Final status: PASS
No Critical, High, or Medium smart-contract vulnerability was identified within the reviewed public-source, ABI, deployed-address, and architecture scope. V6 is appropriate as the primary funding path under the documented hybrid trust model.

The deployed V6 architecture materially improves on a basic hotwallet or proxy-only custody model. It combines a direct non-upgradeable core, registered-wallet withdrawals, event-based slot seasoning, a shared Grouped-Par cap, token-specific liquidity and conditional velocity controls, replay prevention, emergency controls, strict transfer invariants, and a non-authoritative read-only views companion.

Because V6 is hybrid, exact trading, P&L, exposure, token-level netting, and membership-transition allocation remain off-chain. The PASS opinion therefore depends on continued correctness of the publisher/reconciler and privileged-role controls; those private systems and procedures were not audited.

V6 is appropriate as the primary production funding path within the stated public scope. V1 should remain a separately capped, exception-only fallback/hotwallet for narrow, recent deposit-withdraw cases.

This opinion does not certify private engine code, signer custody, organizational controls, solvency, legal compliance, formal verification, or future configuration changes. Dynamic chain state may change after the review date.

Appendix A - Source Evidence Matrix

ID	Source	Location	Audit use
E1	FundingContractV6.sol	Reviewed source package	Core purpose, roles, composites, publication, cap/rate, emergency, withdrawal, membership, and transfer logic.
E2	FundingContractV6Views.sol	Reviewed source package	Read-only companion boundary, immutable core, exports, and duplicated balance resolution.
E3	Ethereum V6 core	https://etherscan.io/address/0xfb41c4f731a064fb3911d16d529be0c2958d5fc6	Core address, public source/ABI, read/write surface, and transaction monitoring.
E4	XDC V6 core	https://xdcscan.com/address/0xfb41c4f731a064fb3911d16d529be0c2958d5fc6	XDC core address, public source/ABI/transaction surface, and chain-specific configuration.
E5	Ethereum V6 views	https://etherscan.io/address/0x228d706e0651038dd8ec151e2f639b3e47ffecb6	Read-only companion address and public source/read surface.
E6	XDC V6 views	https://xdcscan.com/address/0x228d706e0651038dd8ec151e2f639b3e47ffecb6	XDC read-only companion address and public source/read surface.
E7	Ethereum Read Contract	https://etherscan.io/address/0xfb41c4f731a064fb3911d16d529be0c2958d5fc6#readContract	Dynamic admin, role, asset, threshold, composite, publish-state, and views-binding checks.
E8	Ethereum USDT route	https://etherscan.io/token/0xdac17f958d2ee523a2206206994597c13d831ec7?a=0xfb41c4f731a064fb3911d16d529be0c2958d5fc6#transactions	USDT holder/transfer evidence for the V6 core; point-in-time only.
E9	XDC USDC route	https://xdcscan.com/token/0xfa2958cb79b0491cc627c1557f441ef849ca8eb1?a=0xfb41c4f731a064fb3911d16d529be0c2958d5fc6#transactions	XDC USDC holder/transfer evidence for the V6 core; point-in-time only.
E10	V1 fallback proxy	https://etherscan.io/address/0x8815e8F0eb65E1072518e8F842C3aD5199DFCEF1	Fallback/hotwallet proxy identity and monitoring reference.
E11	Polygon PositionManager	https://polygonscan.com/address/0xf857aC7bed76B43c5457f56483803C4CebbD7eff	Positions-only ledger context.
E12	XDC PositionManager	https://xdcscan.com/address/0xf857aC7bed76B43c5457f56483803C4CebbD7eff	Positions-only ledger context.
E13	Prior V5 public audit	https://quote.trade/docs/quote-trade-audit-v5.pdf	Historical V1 fallback and PositionManager context.
E14	Documented production architecture and threshold	Grouped-Par ETH USDC+USDT; Segregated XDC USDC; $1m per-token activation	Production operating assumptions; dynamic on-chain configuration requires continuous verification.

Appendix B - Glossary

Term	Meaning in this report
Composite	Settlement/accounting unit backed by one or more real tokens.
Grouped-Par composite	Two or more approved par-value tokens sharing one published balance and one on-chain cap; Ethereum production design groups USDC and USDT.
Segregated composite	One-token composite that preserves token-specific publication and withdrawal behavior; XDC USDC uses this production pattern.
Low-liquidity threshold	Write-once per-token engine-unit balance below which the 3% hourly and 18% daily aggregate checks are bypassed; production stablecoin policy is $1 million per token.
Slot	Event-bound composite balance observation; qualifying slots are at least 22 hours apart.
capBasis	Seasoned basis from which the 1.5x gross cap is calculated.
capConsumed	Amount already charged against a slot source in the active window.
Provisioning composite	Pre-created target/successor that can receive publications before timelocked activation.
Transition conservation	Engine invariant that aggregate child withdrawal capacity after couple/decouple/merge cannot exceed the parent remaining capacity and cannot strand an offsetting negative leg.
Low-liquidity relief	Configured per-token threshold below which 3%/18% assertions are skipped; all other gates remain.
V1 fallback/hotwallet	Earlier proxy-based Ethereum funding wallet retained only for capped exception use.