Quote.Trade

V5 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**	**2026-06-25**

Scope class	Public smart-contract, public ABI, public explorer metadata, transaction/event sampling, and deployment-posture review.
In-scope V5 funding	Ethereum FundingContractV5 at 0xE430d7906c3D3144223cF2b4d0d2eb16247d6881; XDC FundingContractV5 at 0xE430d7906c3D3144223cF2b4d0d2eb16247d6881.
In-scope V1 fallback	Ethereum TransparentUpgradeableProxy at 0x8815e8F0eb65E1072518e8F842C3aD5199DFCEF1, treated only as constrained fallback/hotwallet.
In-scope position layer	Polygon and XDC PositionManager at 0xf857aC7bed76B43c5457f56483803C4CebbD7eff.
Primary conclusion	V5 should be the primary funding-wallet architecture. V1 should remain capped, monitored, and limited to small, recent deposit-withdraw edge cases only.

Important limitation

This report is not a private-code audit, infrastructure penetration test, signer-custody assessment, formal proof, legal attestation, financial audit, or verification of the proprietary offline engine. It is an audit-style review grounded in public explorer evidence, public ABI/source metadata, and management-provided operating constraints. Ethereum V5 source is exact-match verified; XDC source was not displayed, so XDC conclusions are limited to deployment/activity and supplied-source review.

1. Executive Summary

The reviewed architecture is a hybrid funding and risk-control model. V5 funding contracts custody or account for user funding on the relevant chain, while the publisher/offline engine performs reconciliation, exposure checks, available-balance computation, and withdrawal-risk review before balances are published or withdrawals are approved. The position contracts are treated as positions-only ledger surfaces, not primary funding custody.

Production FundingContractV5 at 0xE430d7906c3D3144223cF2b4d0d2eb16247d6881 supersedes V4 on Ethereum and XDC. Ethereum is exact-match verified; XDC deployment/activity was observed, but XDCScan did not display verified source. V5 retains event-based slots at least 22 hours apart and excludes pre-registration slots from user eligibility; delayed publishing does not reset slots.

V5 retains the 1.5x lowest-slot cap, 18% daily and 3% hourly limits, 10-minute cooldown, three-day emergency freeze, registration-anchored eligibility, replay and liquidity checks, signer rotation, history invalidation, and strict transfer invariants.

V1 remains in scope only as a constrained fallback/hotwallet path. It should be used only when a user deposit is followed by an attempted small withdrawal inside a less-than-3-day window and the request passes reconciliation, risk, V1-cap, and approval checks. V1 should not be used as a parallel primary funding wallet or as a default withdrawal path.

Executive opinion

PASS - public smart-contract and public-explorer scope. No Critical, High, or Medium smart-contract issue was identified. Production V5 initialization and balance publishing were observed; no live V5 withdrawal was sampled. The PASS conclusion depends on V1 fallback limits and publisher/offline-engine controls.

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.
Low	0	PASS	No Low code-level issue was separated from informational operating requirements in this public review.
Informational	6	Accepted / mitigated by design	Informational items document architectural dependencies, operating requirements, and residual trust assumptions.

Key conclusion	Assessment
V5 primary funding	Appropriate primary architecture based on reviewed public ABI/deployment posture and expanded controls.
V5 non-upgradeability posture	Ethereum public explorer evidence identifies V5 as exact-match verified FundingContractV5 rather than a V1-style TransparentUpgradeableProxy. XDC production deployment/activity was observed separately; XDCScan source verification was not displayed at the review date.
V1 fallback/hotwallet	Acceptable only if capped, monitored, and constrained to small, recent deposit-withdraw edge cases under independent approval.
Publisher/offline engine	Security-critical part of the architecture. It must be treated as a production control plane with deterministic logs, reconciliation, alerting, and independent review.
PositionManager layer	Suitable as a positions-only ledger surface if freshness, batch-completeness, and mapping-change controls are monitored continuously.

2. Scope, Methodology, and Review Boundaries

This review follows the public-audit style of the existing Quote.Trade audit while expanding the analysis to the V5 funding contracts, the V1 fallback/hotwallet policy, and the XDC position/funding footprint. The prior public report expressly framed the review as public-source, code-only, and not a test of off-chain matching, pricing, liquidation, signer infrastructure, private repositories, deployment operations, or organizational controls. This report uses the same boundary and makes the hybrid dependencies explicit.

In-scope item	Networks / assets	Purpose in this review
V5 funding contracts	Ethereum Mainnet USDC/USDT; XDC Network USDC	Primary funding-wallet architecture and V5 control assessment.
V1 funding contract	Ethereum Mainnet USDC/USDT	Fallback/hotwallet only; proxy and operational risk assessment.
PositionManager contracts	Polygon and XDC	Positions-only ledger and publisher/batch freshness assessment.
Explorer metadata	Etherscan, PolygonScan, XDCScan	Contract identity, Ethereum verified source/ABI, XDC deployment/activity and source-verification status, proxy posture, and transaction/event sampling.
Management-provided constraints	V5 primary; V1 fallback only for small + recent deposit-withdraw cases	Architecture and operating-policy assumptions used in the PASS opinion.

Out-of-scope item	Implication
Private source code or internal repositories	Not reviewed; this report cannot prove unpublished logic.
Offline engine implementation, databases, APIs, matching, pricing, liquidation, market-risk logic	Treated as a security-critical assumption and operating dependency.
Signer custody, multisig configuration, key generation, KMS, hardware wallet procedures	Assumed secure; monitoring and governance recommendations are provided.
Formal verification, fuzzing, symbolic execution, line-by-line private-code audit	Not performed in this public-scope report.
Legal, compliance, accounting, proof-of-reserves, or solvency attestation	Not covered; token balances are point-in-time context only.

Methodology

1. Review public explorer pages for contract identity, source-code verification metadata, proxy posture, ABI/function names, and recent transaction methods.
2. Map public ABI controls and custom errors to risk classes: stale balances, batch incompleteness, over-withdrawal, duplicate withdrawals, role compromise, liquidity risk, and emergency containment.
3. Compare V5 direct FundingContractV5 posture against V1 TransparentUpgradeableProxy posture and identify governance/upgrade-risk differences.
4. Evaluate the hybrid design assumptions: publisher/offline reconciliation, available-balance publication, position-ledger freshness, and fallback routing policy.
5. Document findings using a formal audit style: severity, status, affected components, evidence, impact, recommendation, and residual risk.

Management-provided operating constraints incorporated

V5 is treated as the primary funding wallet architecture. V1 is treated only as a fallback/hotwallet path for cases where a user deposits and attempts to withdraw a small amount within less than 3 days, subject to reconciliation, risk, approval, and V1 cap checks. These constraints are operating assumptions and should be encoded in policy, monitoring, and runbooks.

3. Contract Inventory and Deployment Posture

The inventory separates primary funding custody, fallback/hotwallet custody, and positions-only ledger surfaces. This distinction is important because the risk profile of a funding wallet differs materially from a position-publication contract.

ID	Component	Network	Address	Explorer identity / posture	Architecture role
F-V5-ETH	V5 funding	Ethereum	0xE430d7906c3D3144223cF2b4d0d2eb16247d6881	FundingContractV5; exact-match verified source metadata; public page shows Code / Read / Write rather than V1 proxy tabs. Evidence: E2.	Primary V5 funding wallet for Ethereum USDC / USDT funding.
F-V5-XDC	V5 funding	XDC	0xE430d7906c3D3144223cF2b4d0d2eb16247d6881	FundingContractV5 production deployment; XDCScan source was not verified at the review date, but public transactions show role configuration, asset configuration, user registration, and balance publication. Evidence: E3.	Primary V5 funding wallet for XDC USDC funding.
F-V1-ETH	V1 fallback	Ethereum	0x8815e8F0eb65E1072518e8F842C3aD5199DFCEF1	TransparentUpgradeableProxy; proxy tabs and implementation indirection visible. Evidence: E4.	Fallback/hotwallet only; not primary funding.
P-POL	PositionManager	Polygon	0xf857aC7bed76B43c5457f56483803C4CebbD7eff	PositionManager; verified source; frequent batchUpdatePositions. Evidence: E5.	Positions-only ledger / publisher state surface.
P-XDC	PositionManager	XDC	0xf857aC7bed76B43c5457f56483803C4CebbD7eff	PositionManager; verified source; frequent batchUpdatePositions. Evidence: E6.	Positions-only ledger / publisher state surface.

4. Hybrid Architecture and Reconciliation Flow

The architecture is intentionally hybrid. On-chain funding contracts should not be read as a complete on-chain trading, matching, liquidation, or margin engine. Instead, the publisher/offline engine acts as the reconciliation and risk-control layer that computes safe available balances, validates withdrawal eligibility, and publishes only approved state to the chain.

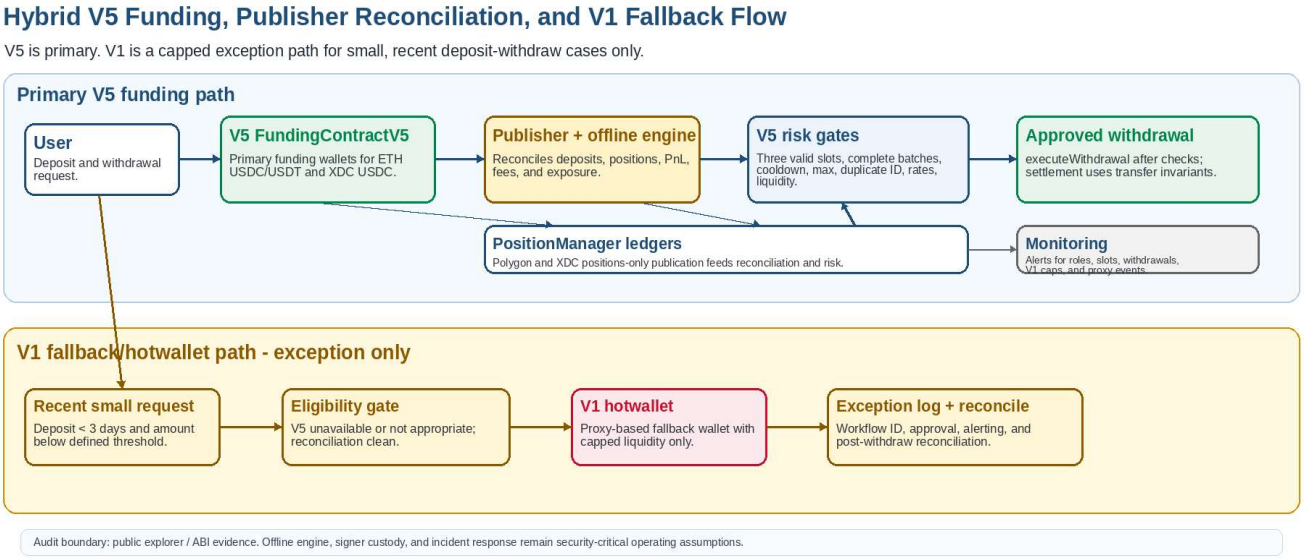

Figure 1. Hybrid V5 primary funding architecture with V1 fallback/hotwallet exception path.

Required reconciliation and risk checks before V5 withdrawal

Control step	Purpose	Minimum evidence / audit trail
Deposit recognition	Confirm deposits by token, chain, contract address, user mapping, amount, and block finality.	On-chain transfer hash; off-chain deposit ledger entry; reconciliation batch ID.
User and asset mapping	Ensure the userId, wallet, asset address, symbol, decimals, and engine scale are consistent.	Mapping version; asset config version; exception log if changed.
Position and exposure reconciliation	Reconcile fills, open positions, realized/unrealized PnL, fees, funding, collateral, and prior withdrawals.	Offline engine calculation record; signed publisher snapshot; reviewer ID.
Snapshot completeness	Prevent withdrawal decisions from stale, incomplete, duplicate, or gap-filled batches.	Snapshot ID; batch index count; freshness timestamp; stale/gap alerts.
Withdrawal eligibility	Confirm cooldown, max withdrawable, liquidity, duplicate-withdrawal status, rate limits, and emergency mode state.	Risk-check result; withdrawal approval record; withdrawalId.
Fallback eligibility	Only route to V1 if small amount, deposit age < 3 days, clean risk result, V1 cap, and independent approval all pass.	V1 exception record; small-threshold check; V1 cap dashboard; post-withdraw reconciliation.

5. V5 FundingContract Deep Review

V5 FundingContractV5 is the primary funding-security deployment. The reviewed Ethereum exact-match source exposes constants and checks for three event-based balance slots, registration-anchored user eligibility, a 1.5x user cap, 18% daily and 3% hourly asset drain limits, a 10-minute publish cooldown, a 22-hour minimum between qualifying commits, a 3-day emergency freeze, balance and amount caps, role separation, exact-trigger emergency history invalidation, and strict ERC-20/native transfer invariants. Slot history is not reset by a delayed or missed calendar-day publication.

Positive observation	Security value	Evidence / notes
Direct FundingContractV5 deployment posture	Reduces proxy-admin upgrade risk relative to V1 fallback proxy posture.	E2 identifies the Ethereum V5 address as exact-match verified FundingContractV5; E3 identifies the corresponding XDC production deployment, with source verification not displayed at the review date.
Role-separated control plane	Limits the blast radius of any single operational function and makes role changes observable.	V5 ABI includes balance-poster, withdrawal, guardian, and role grant/revoke functions/events.
Snapshot-aware balance publication	Protects against stale, skipped, incomplete, duplicate, or misaligned publisher data.	The verified V5 ABI includes snapshot ID, batch count, duplicate batch, stale/gap, event-based slot cadence, and pending snapshot controls.
Withdrawal hard gates	Withdrawal execution is bounded by on-chain conditions in addition to off-chain approval.	V5 ABI includes max-withdrawable, cooldown, duplicate-withdrawal, liquidity, and rate-limit controls.
Emergency and signer rotation controls	Provides containment and rotation signals during abnormal conditions.	V5 ABI includes emergency-mode functions/events and signer-rotation conditions.
Token/native transfer invariants	Detects fee-on-transfer or unexpected debit/credit behavior and prevents silent accounting drift.	V5 ABI includes token and native transfer invariant errors.
On-chain observability	Enables independent monitoring of role, snapshot, withdrawal, and emergency events.	Recent public transactions include role grants, asset configuration, user registration, and Batch Set Available calls on Ethereum and XDC V5. No V5 withdrawal was sampled at the review date because the deployments were newly initialized.

5.1 V5 funding protections

Protection	How it reduces risk
Stablecoin-only funding policy	In-scope production funding routes are Ethereum USDC, Ethereum USDT, and XDC USDC. Non-stable asset routes are out-of-scope unless separately reviewed.

Protection	How it reduces risk
Registered-wallet withdrawal path	Users are registered by userId and wallet address. executeWithdrawal sends funds to the user address; there is no separate arbitrary recipient field. Engine/reconciler must enforce deposit wallet equals withdrawal wallet.
Registration-anchored slot eligibility	Registration time anchors the eligible slot history. Asset slots committed before the user was registered are excluded from the three-slot withdrawal test. There is no separate fixed-duration registration timer; a fresh three-slot sequence can complete in approximately 44 hours, followed by the 10-minute cooldown, and may take longer depending on registration timing.
3 committed event-based balance slots	Withdrawals require three committed slot identities in the asset ring. Slots do not need to fall on consecutive calendar days, and a delayed publication does not reset previously qualified slots.
At least 22 hours between qualifying slot commits	A completed publication at least SNAPSHOT_COMMIT_MIN_INTERVAL after the previous qualifying commit advances the slot ring; an earlier completed publication is a same-slot correction. The reviewed source sets the interval to 22 hours and imposes no maximum gap.
Batch integrity	Batch publishing uses snapshotId, batchIndex, totalBatches, body alignment checks, sequential snapshot ID enforcement, total-batch consistency, and duplicate batch-index prevention. The first nonzero snapshotId for a never-published asset may establish its starting value; strict +1 sequencing applies thereafter.
Pending snapshot withdrawal block	If a non-final snapshot is pending, withdrawals for that asset are blocked until the run commits or the pending state is cleared by the defined recovery rules.
10-minute post-publish cooldown	Every committed publish refreshes lastPublishTime. Withdrawals remain blocked for WITHDRAWAL_COOLDOWN, which is 10 minutes in the reviewed source.
Lowest-slot 1.5x user cap	The user-level ceiling is the minimum remaining cap across the three-slot window. Each slot is capped at NORMAL_MULTIPLIER_BPS = 15,000 / 10,000 = 1.5x the effective cap basis.
Cap consumption and carry-forward handling	Withdrawals charge capConsumed against unique source slots in the active window and apply aged capBasis rules to prevent stale cap room from surviving when the source leaves the window.
Zero publish hard-close	Publishing zero for a user+asset hard-closes the slot by wiping balance, capBasis, and capConsumed. A fresh non-zero publish is required to reopen availability.
MAX_BALANCE one-slot bound	Published balances and withdrawal amounts are capped so the gross 1.5x cap fits in uint64 while preserving the packed one-slot UserSlot design.
Replay protection	processedWithdrawals records each withdrawalId. A duplicate withdrawalId cannot execute twice.
Contract liquidity check	Before transfer, the contract checks actual token/native balance and rejects withdrawals above available contract liquidity.
Asset drain limits	Asset-level daily withdrawals are capped at 18% and hourly withdrawals at 3% of the engine-scale pool base for that window. These limits are shared by all users of the asset.
Strict transfer invariant	ERC-20 transfers require exact contract debit and exact recipient credit. Native transfers require exact contract debit. Fee-on-transfer/rebasing behavior is rejected.
Reentrancy and CEI	executeWithdrawal is nonReentrant and performs state effects before the external transfer.
Emergency freeze	Emergency mode blocks withdrawals and new user registrations for 3 days while allowing recovery publication after key rotation.
Emergency history floor	Emergency sets balanceHistoryFloor to the exact trigger timestamp so pre-trigger history cannot be used for clean recovery.
Emergency key rotation	Emergency increments signerRotationEpoch and forces balance-poster and withdrawal keys to be re-granted under the new epoch before they work again. This is designed for hacked publisher/withdrawal key response.
Guardian response path	Admin or guardian can activate emergency. Guardians remain available as freeze operators even though poster and withdrawal keys must rotate.

Protection	How it reduces risk
Observability	Events expose role changes, user registration, balance updates, slot commits, withdrawals, emergency activation, signer rotation, history invalidation, and recovery completion.

5.2 V5 withdrawal gating sequence

A V5 stablecoin withdrawal must pass all of the following before funds leave the contract:

1. Asset is supported under the stablecoin funding policy.
2. User address is nonzero and registered; all three counted cap entries must correspond to asset slots committed at or after the user's registration timestamp.
3. Emergency mode is inactive.
4. withdrawalId is nonzero and has not been processed before.
5. The asset has a committed slot identity and a fully populated three-slot ring.
6. No pending valid snapshot exists for the asset.
7. The latest completed publication is committed; no incomplete multipart snapshot remains.
8. 10-minute post-publish cooldown has expired.
9. Three committed slots exist, and adjacent qualifying commit times are at least 22 hours apart; calendar-day gaps do not reset prior slots.
10. User has three valid cap entries corresponding to the active three-slot ring.
11. Requested amount is no greater than the user's minimum remaining cap across the three-slot window.
12. Contract has sufficient token liquidity.
13. Asset-level 3% hourly and 18% daily withdrawal caps are not exceeded.
14. State updates, rate-limit accounting, cap consumption, and processed withdrawal ID are recorded before transfer.
15. The transfer succeeds with exact debit/credit invariant checks.

5.3 Emergency-mode design

Emergency mode is designed for compromise response, especially publisher or withdrawal-key compromise. Triggering emergency always resets the freeze to three days from the current trigger time, raises the balance-history floor to the exact trigger timestamp, and increments signerRotationEpoch. Any poster or withdrawal key granted under the old epoch stops working until explicitly re-granted. This forces a fresh key rotation path before publication or withdrawals can resume.

Clean recovery requires three post-floor committed slots with at least 22 hours between qualifying commits. The freeze period and clean-recovery window run concurrently; withdrawals can resume only when the three-day freeze has ended and the asset has three valid post-floor slots. Emergency does not destroy historical data; it makes pre-floor entries unusable until clean balances are republished.

5.4 V5 limitations accepted under the hybrid model

Limitation / dependency	Treatment in audit
Engine and reconciler are security-critical	Accepted. Exact balance/risk truth and stale-state authority are off-chain by design. The contract preserves qualified slots across publication gaps; the engine remains responsible for freshness and dirty-user blocking.
After a withdrawal, user+asset must be dirty until reconciled	Required operating invariant. The engine must republish updated balance/zero or block future V5 withdrawals for that user+asset.
Publisher omissions are operationally invalid when they hide withdrawals	Accepted as reconciler responsibility. Omitted unchanged users are supported; omitted dirty users are not a valid production path.
Abandoned write-bearing snapshot runs are reconciler-managed	Accepted. Sequential snapshot IDs and pending state reduce risk, but the reconciler must pause or verify any abandoned write-bearing publish.
V5 views are guardrails, not authorization	Accepted. getMaxWithdrawable is the on-chain ceiling; the withdrawal engine must still perform exact engine checks.

5.5 V5 control themes

- Available balances are not treated as arbitrary administrator entries. The ABI shows snapshot, slot-cadence, and batch guardrails that require structured publication and complete multipart updates.
- Withdrawals are not just off-chain approvals. The contract can enforce maximum withdrawable amounts, cooldowns, per-asset withdrawal-rate limits, sufficient contract liquidity, duplicate-withdrawal prevention, and emergency-mode blocking.
- Operational roles are separated. Balance publication, withdrawal execution, guardian/emergency response, and administration have distinct functions and observable role events.
- V5 non-upgradeability is a security tradeoff. It removes the proxy-admin upgrade path from the primary funding wallet posture, but future changes require a controlled migration rather than in-place patching.

V5 conclusion

V5 is appropriate as the primary funding-wallet architecture under the public-scope assumptions reviewed. The protections materially reduce the risk profile relative to relying on a proxy-based V1 hotwallet as the primary custody surface.

6. Non-Upgradeability and V5 vs. V1 Comparison

The report treats V5 as non-upgradeable based on public deployment posture and the exact-match verified Ethereum source: the Ethereum funding page identifies FundingContractV5 and does not present a proxy surface. The XDC deployment uses the same production address and shows matching initialization/publication methods, but XDCScan did not display verified source at the review date. The V1 address remains an explicit TransparentUpgradeableProxy. This is a public-evidence deployment-posture conclusion, not a private deployer attestation.

Check	V5 Ethereum funding	V5 XDC funding	V1 Ethereum fallback	Security implication
Explorer contract identity	FundingContractV5 (E2)	FundingContractV5 deployment (E3; source not verified on XDCScan)	TransparentUpgradeableProxy (E4)	V5 avoids the visible V1 proxy-admin identity.
Proxy tabs / implementation indirection	No V1-style Read as Proxy / Past Implementations posture observed in reviewed page.	No V1-style proxy posture was observed. XDCScan source equivalence was not independently verified at the review date.	Read as Proxy, Write as Proxy, Past Implementations, and Implementation are visible (E4).	V1 requires proxy-admin monitoring and upgrade governance; V5 primary funding reduces that attack surface.
Upgrade ABI surface	No upgradeTo / upgradeToAndCall observed in the reviewed V5 source/ABI evidence.	No upgradeTo / upgradeToAndCall observed in the reviewed V5 source/ABI evidence.	Proxy ABI exposes upgrade-related events and proxy fallback structure (E4).	V5 primary funding avoids routine proxy-upgrade risk; V1 remains an operational trust surface.
Change-management model	Migration required for new V5 code.	Migration required for new V5 code.	Proxy implementation may be changed by proxy governance.	V5 reduces unauthorized upgrade risk but increases need for safe migration procedures.
Monitoring priority	Role, withdrawal, snapshot, and emergency monitoring.	Role, withdrawal, snapshot, and emergency monitoring.	All V5-style monitoring plus AdminChanged, Upgraded, implementation changes, and V1 balance caps.	V1 should be restricted to capped fallback only.

V5 vs. V1 risk posture

Risk area	V5 primary funding posture	V1 fallback/hotwallet posture	Audit treatment
Upgrade/governance risk	Direct FundingContractV5 posture; no proxy-admin path observed in reviewed public ABI.	TransparentUpgradeableProxy with implementation indirection.	V5 materially improves governance risk; V1 must be capped and monitored.
Withdrawal controls	Cooldown, max-withdrawable, duplicate-withdrawal, rate-limit, liquidity, and emergency checks visible in ABI.	Earlier V1 custody model depends on the proxy implementation and prior controls.	V5 should process normal withdrawals; V1 only exception path.
Publisher model	Batch set available balances with V5 snapshot/batch protections.	V1 should not be used as primary available-balance publisher for normal flow.	Publisher correctness remains critical across both.
Incident containment	Guardian/emergency mode and role revocation controls visible.	Proxy and fallback cap monitoring required.	V5 has stronger on-chain containment; V1 relies more on operational caps.
Operational complexity	Higher V5 control richness; more alerts and runbooks required.	Simpler hotwallet-style fallback, but higher upgrade/custody risk.	Operational burden is acceptable if V1 remains bounded.

7. Role and Permission Matrix

The hybrid model is secure only if privileged roles and off-chain actors are treated as production security controls. The table below maps expected capabilities, compromise impact, and required mitigations.

Actor / role	Expected capability	Abuse or failure risk	Required mitigation
Admin / owner	Configure supported assets, grant/revoke roles, manage high-impact settings.	Privilege escalation, unsafe configuration, unauthorized role creation, asset misconfiguration.	Multisig or equivalent institutional control; two-person approval; change tickets; real-time role/config alerts.
Balance poster / publisher role	Publish available balances and snapshots after offline reconciliation.	Incorrect balances, stale data, incomplete snapshots, manipulated availability.	Deterministic reconciliation logs; snapshot completeness checks; independent monitoring; anomaly thresholds.
Withdrawal role	Execute approved withdrawals on V5.	Unauthorized withdrawal if approval workflow fails or role is compromised.	Independent approval; withdrawalId uniqueness; per-asset limits; post-withdraw reconciliation; emergency block path.
Guardian	Activate emergency mode and support rapid containment.	Improper pause/activation, delayed incident response, or overuse.	Dedicated incident runbook; dual-control activation; post-incident review and rotation.
Publisher/offline engine	Compute reconciled balances, risk state, exposure, PnL, and eligibility.	Centralized correctness dependency; corrupted data can affect published balances.	Deterministic replay; signed batch artifacts; independent risk review; exception queues; immutable logs.
Position updater	Publish position batches to PositionManager contracts.	Stale or incomplete position state; incorrect mappings.	Sync-frequency dashboard; processed/total batch checks; mapping-change alerts; rollback/recovery playbook.
V1 proxy admin / upgrade authority	Ability to control proxy implementation where applicable.	V1 implementation change or admin abuse could affect fallback funds.	Monitor AdminChanged, Upgraded, implementation changes; keep V1 balances capped; require emergency withdrawal halt.
Monitoring / sentinel	Observe events and trigger alerts.	Missed role changes, stale snapshots, abnormal withdrawal patterns.	24/7 alerts; escalation SLAs; false-positive review; periodic test incidents.

8. Security Control Mapping

This table maps the main V5 protections to the risk they mitigate. Controls observed in public ABI/explorer evidence must be complemented by operational enforcement in the publisher/offline engine.

Risk class	V5 protection / observed control family	Purpose	Operating requirement
Fast deposit-withdraw abuse	WithdrawalCooldownActive; registration-anchored three-slot cadence; offline deposit-age policy	Prevents immediate extraction before three reconciled balance observations and the post-publish cooldown.	Define age gates and manual-review triggers; V1 only for small, approved <3-day exceptions.
Over-withdrawal	ExceedsMaxWithdrawable; getMaxWithdrawable; min-valid balance model	Prevents withdrawals above reconciled availability.	Recompute max withdrawable off-chain and compare against on-chain result.
Duplicate / replayed withdrawal	processedWithdrawals; WithdrawalAlreadyProcessed; unique withdrawalId	Prevents the same withdrawal from executing twice.	Withdrawal IDs must be deterministic and collision-resistant; alert on duplicate attempts.
Asset drain / velocity risk	ASSET_HOURLY_WITHDRAWAL_LIMIT_BPS; ASSET_DAILY_WITHDRAWAL_LIMIT_BPS; ExceedsAssetWithdrawalRateLimit	Limits outflow even if an approval process fails.	Set alert thresholds below hard limits; monitor hourly and daily aggregate outflows.
Liquidity mismatch	InsufficientContractLiquidity; getContractBalance	Blocks withdrawals when contract lacks sufficient token/native balance.	Treasury dashboard comparing reconciled liabilities, contract balances, and expected hotwallet caps.
Stale or incomplete balance data	StaleSnapshotId; SnapshotIdGap; SnapshotUpdatePending; InsufficientSnapshots	Blocks gapped IDs, incomplete multipart updates, or insufficient slot history. A missed calendar day alone does not invalidate existing slots.	Monitor publication age and dirty-user state off-chain; alert on pending batches, ID gaps, and unusually long publication gaps.
Malformed or incomplete batches	BatchCountMismatch; BatchBodyMisaligned; BatchIndexOutOfRange; DuplicateBatchIndex	Protects against incomplete or corrupted publisher payloads.	Publisher should pre-validate batches and retain signed payload artifacts.
Emergency containment	activateEmergencyMode; EmergencyModeActive; EmergencyModeActivated / Expired	Enables rapid containment during incidents.	Document who can activate, how to notify users, and how to resume safely.
Signer / role hygiene	SignerRotationRequired; SignerKeyNotRotated; role grant/revoke events	Forces attention to role rotation after incident or expiry.	Test signer rotation periodically and log every grant/revoke.
Token behavior anomalies	SafeERC20FailedOperation; TokenTransferInvariantFailed; NativeTransferInvariantFailed	Detects unexpected token/native transfer behavior.	Test every supported asset; avoid unreviewed fee-on-transfer or rebasing assets.
Asset configuration risk	setSupportedAsset; AssetConfigured; InvalidTokenDecimals; InvalidEngineScale	Prevents mismatched asset, decimal, or engine-scale configuration.	Require two-person review for asset configuration and decimals.

9. V1 Fallback/Hotwallet Review

V1 is not treated as the primary funding architecture. The Ethereum V1 address is identified publicly as a TransparentUpgradeableProxy, and therefore carries a different upgrade-governance and hotwallet risk posture than V5. The appropriate use of V1 is a tightly constrained fallback/hotwallet path for small, recent deposit-withdraw edge cases only.

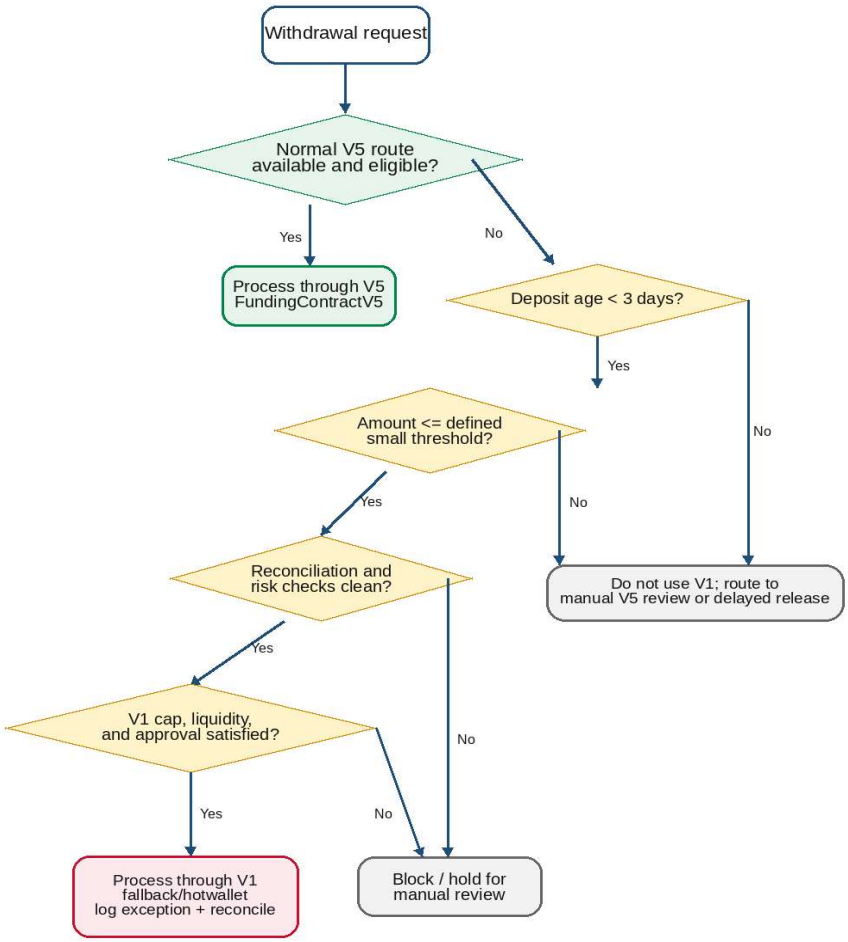

Figure 2. Required V1 fallback/hotwallet decision tree.

Fallback condition	Required interpretation
Deposit age less than 3 days	A maximum eligibility condition for edge cases, not a default withdrawal SLA. Requests older than the defined window should not use V1 fallback.
Small amount	Must be numerically defined per asset, per user, and per rolling window before production reliance. Without numbers, this control is not audit-enforceable.
Clean reconciliation and risk checks	The offline engine must confirm no suspicious activity, no exposure mismatch, no unresolved chargeback/funding risk, and no stale balance state.
V5 route unavailable or not appropriate	V1 should be used only when normal V5 processing cannot safely or efficiently handle the case.
V1 balance cap and liquidity	V1 must hold only capped operational liquidity sized to fallback needs, not platform-wide liabilities.
Independent approval and logging	Every V1 fallback withdrawal must record user, asset, amount, deposit time, reason, approver, workflow ID, and post-withdraw reconciliation.

V1 conclusion

The V1 fallback/hotwallet path is acceptable only as a tightly capped exception path. It should be excluded from normal funding-wallet 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 are reviewed as positions-only ledger and withdrawal-request/event surfaces. They are not primary funding wallets in this report. The key security question is whether position publication is fresh, complete, and controlled by authorized updaters.

Observation	Polygon PositionManager	XDC PositionManager	Audit significance
Contract identity	PositionManager (E5)	PositionManager (E6)	Confirms positions-layer role rather than V5 funding wallet role.
Recent activity	Frequent batchUpdatePositions transactions observed.	Frequent batchUpdatePositions transactions observed.	Supports active publisher flow and need for freshness monitoring.
Roles	Public ABI/source indicate role-based updater/admin controls.	Public ABI indicates ADMIN_ROLE and UPDATER_ROLE.	Role changes and updater address must be monitored.
Freshness and batch model	processedBatches, totalBatches, lastSyncedTime, and syncFrequency style controls are core to the position layer.	ABI exposes syncFrequency, lastSyncedTime, snapshotId, totalBatches, processedBatches functions.	Withdrawal/risk decisions should reject stale or incomplete position state.
Custody posture	Treated as positions-only and non-custodial.	Treated as positions-only and non-custodial.	Do not market this layer as a funding or custody contract.

Position-layer risk	Required control
Stale position publication	Alert when lastSyncedTime exceeds the allowable syncFrequency window.
Incomplete batch publication	Block dependent withdrawal/risk decisions unless processedBatches equals totalBatches for the active snapshot.
Unauthorized updater changes	Alert on role changes and require operational approval records.
Mapping inconsistency	Alert on user and asset registration/update functions; treat mapping changes as production change events.
Misinterpretation of withdraw()	Document whether withdraw() is a request/event path and not token custody transfer for the positions layer.

11. Transaction and Event Sampling

The following samples are not a complete transaction audit. They demonstrate the type of public activity reviewed and the monitoring categories that should be automated.

Category	Network / contract	Representative public evidence	Audit use
V5 available-balance publication	Ethereum V5 funding (E2)	Recent Batch Set Available... transactions include tx 0x1772e928... at block 25392948 and tx 0x05acde83... at block 25392945.	Supports the architecture where publisher/balance-poster updates available balances.
V5 XDC balance publication	XDC V5 funding (E3)	Batch Set Available... transaction observed at tx 0xcf6c0c77... at block 104184729, with subsequent publication activity.	Confirms XDC V5 publisher activity.
V5 withdrawal execution status	Ethereum/XDC V5 funding (E2/E3)	No executeWithdrawal transaction was observed in the sampled new V5 deployment activity at the review date; the withdrawal path was reviewed from the exact-match verified Ethereum source.	Live withdrawal behavior had not yet been demonstrated on-chain in the sampled deployment window.
V5 role/configuration changes	Ethereum and XDC V5 funding (E2/E3)	Grant Guardian, Grant Balance Poster, Grant Withdrawal Role, and Set Supported Asset transactions were observed on Ethereum around blocks 25391125-25391151 and on XDC around blocks 104177205-104177215.	Supports role/config monitoring recommendations.
Polygon position updates	Polygon PositionManager (E5)	Frequent Batch Update Pos... transactions, including tx 0x32244207... at block 88512599 and many 10-minute cadence examples.	Supports position-publisher freshness analysis.
XDC position updates	XDC PositionManager (E6)	Frequent Batch Update Pos... transactions, including tx 0xe158ed2f... at block 103787031.	Supports XDC position-publisher freshness analysis.
V1 proxy posture	Ethereum V1 fallback (E4)	Contract creation and proxy metadata observed; contract name TransparentUpgradeableProxy with implementation indirection.	Supports treating V1 as fallback/hotwallet rather than primary funding.

12. Formal Findings

No Critical, High, or Medium vulnerability was identified within the public smart-contract and public-explorer scope. The following informational findings document accepted dependencies, operational requirements, and residual risks that must remain controlled for the PASS opinion to hold.

QT-INFO-01: Hybrid architecture depends on publisher/offline reconciliation correctness

Field	Assessment
Severity	Informational / Operational dependency
Status	Accepted; mitigated by design and required operating controls
Affected components	V5 funding contracts, PositionManager, offline engine, publisher
Description	The architecture relies on off-chain reconciliation and risk checks before available balances are published and withdrawals are approved.
Impact	If the publisher/offline engine publishes stale or incorrect balances, on-chain contracts may enforce bounds around incorrect inputs rather than the true user risk state.
Evidence	Batch Set Available and Batch Update Positions activity; V5 snapshot/batch ABI controls; management-provided hybrid model.
Recommendation	Maintain deterministic reconciliation, signed batch artifacts, independent risk review, stale-snapshot blockers, anomaly alerts, and replayable logs.
Residual risk	Operational correctness remains a residual trust assumption.

QT-INFO-02: V5 privileged roles are security-critical

Field	Assessment
Severity	Informational / Operational dependency
Status	Accepted; mitigated by design and required operating controls
Affected components	Admin, balance poster, withdrawal role, guardian
Description	V5 improves role separation, but the roles remain high-impact production controls.
Impact	A compromised role may publish incorrect balances, execute unauthorized withdrawals, or fail to respond to emergencies.
Evidence	Public V5 ABI exposes role grants/revocations, balance-poster functions, withdrawal functions, and guardian/emergency functions.
Recommendation	Use multisig/equivalent controls, hardware-backed keys, two-person approval, role-change alerts, regular signer rotation, and incident runbooks.
Residual risk	Key-management controls were not directly verified in this public-scope review.

QT-INFO-03: V5 non-upgradeability reduces proxy risk but requires migration governance

Field	Assessment
Severity	Informational / Operational dependency
Status	Accepted; mitigated by design and required operating controls
Affected components	V5 FundingContractV5 on Ethereum and XDC
Description	The Ethereum public explorer posture supports a direct exact-match verified FundingContractV5 deployment rather than a V1-style proxy posture.
Impact	Unauthorized proxy upgrade risk is materially reduced for V5 primary funding, but bugs cannot be patched in place without migration.
Evidence	E2 identifies exact-match verified Ethereum FundingContractV5; E3 identifies the production XDC deployment/activity; E4 identifies V1 as TransparentUpgradeableProxy.
Recommendation	Maintain migration runbooks, user notices, dual-control migration approvals, pause conditions, and reconciliation checkpoints before migrating funds.
Residual risk	Ethereum source is exact-match verified. XDC source was not independently verified on XDCScan at the review date, so XDC source equivalence remains a deployment-assurance assumption.

QT-INFO-04: V1 fallback/hotwallet must remain capped and constrained

Field	Assessment
Severity	Informational / Operational dependency
Status	Accepted; mitigated by design and required operating controls

Field	Assessment
Affected components	V1 Ethereum fallback/hotwallet
Description	V1 is upgradeable and should not be used as a parallel primary wallet. It should only handle small, recent deposit-withdraw exceptions.
Impact	If V1 accumulates material balances or becomes a default withdrawal route, the architecture reintroduces avoidable proxy and hotwallet risk.
Evidence	E4 proxy identity; management-provided V1 fallback policy; V1 token-holder pages E10/E11.
Recommendation	Define hard per-asset caps, threshold-based alerts, withdrawal exception logging, less-than-3-day policy enforcement, and proxy event monitoring.
Residual risk	Fallback use can drift without dashboards, approvals, and independent reviews.

QT-INFO-05: PositionManager correctness depends on timely batch publication

Field	Assessment
Severity	Informational / Operational dependency
Status	Accepted; mitigated by design and required operating controls
Affected components	Polygon and XDC PositionManager
Description	Position contracts are positions-only ledger surfaces, and downstream risk decisions depend on timely and complete publisher updates.
Impact	Stale or incomplete positions may lead to incorrect user balances, margin/risk decisions, or withdrawal eligibility decisions.
Evidence	E5/E6 PositionManager identity and frequent batchUpdatePositions activity.
Recommendation	Maintain lastSyncedTime/syncFrequency dashboards, processed-vs-total batch alerts, mapping-change alerts, and stale-data blockers.
Residual risk	Position freshness is an operational dependency rather than a fully on-chain guarantee.

QT-INFO-06: "Small amount" fallback threshold must be numerically defined

Field	Assessment
Severity	Informational / Operational dependency
Status	Accepted; mitigated by design and required operating controls
Affected components	V1 fallback policy and withdrawal operations
Description	The fallback policy relies on a qualitative "small amount" threshold that must become a quantitative control.
Impact	Without per-asset and per-user numeric thresholds, reviewers cannot determine whether V1 use is compliant or detect policy drift automatically.
Evidence	Management-provided fallback policy; V1 hotwallet design requirements.
Recommendation	Define per-withdrawal, per-user/day, per-asset/day, and total V1 hotwallet caps; include automated blocks and escalation thresholds.
Residual risk	Residual risk is low if numeric caps are enforced and reviewed; higher if thresholds remain informal.

13. Governance, Key-Management Assumptions, and Residual Risks

The PASS conclusion assumes that the privileged accounts and operational workflows behind the public contracts are implemented with institutional controls. This public review could not verify private signer custody or the internals of the offline engine.

Assumption	Required implementation
Privileged accounts are secured	Admin, guardian, balance-poster, withdrawal, updater, and V1 proxy-admin roles should be held by multisig or equivalent institutional controls.
Role changes are monitored	Every grant/revoke or proxy-admin change should produce real-time alerts and require ticketed approvals.
Withdrawal execution has independent approval	The withdrawal role should not be able to approve and execute withdrawals without off-chain risk approval and audit logs.
Offline engine is deterministic and replayable	Reconciliation outputs should be reconstructable from inputs, with signed or immutable batch artifacts.
Emergency procedures are rehearsed	Guardian activation, role revocation, V1 cap reduction, withdrawal pause, and recovery paths should be tested periodically.

Residual risk	Why it remains	Required owner
Offline reconciliation correctness	The private engine cannot be fully verified from public explorer data.	Engineering / Risk
Privileged signer compromise	Public ABI cannot prove custody procedure or signer hardware controls.	Security / Operations
V1 fallback misuse	V1 is upgradeable and hotwallet-style by design.	Treasury / Operations
Stale position publication	PositionManager depends on timely publisher updates.	Publisher / Monitoring
Asset mapping or decimal mismatch	Hybrid systems depend on exact asset address, symbol, and engine-scale consistency.	Engineering / Controls
Migration risk	V5 non-upgradeability requires controlled migration for future changes.	Engineering / Governance
Monitoring gaps	Controls are only effective if alerts are configured, tested, and escalated.	Security Operations

14. Recommendations and Operating Requirements

The following requirements are not blockers to the PASS conclusion, but they should be treated as production operating controls for the hybrid model.

V5 primary funding requirements

- Alert on all role changes: RoleGranted, RoleRevoked, grantBalancePoster, grantWithdrawalRole, grantGuardian, revokeBalancePoster, revokeWithdrawalRole, and revokeGuardian.
- Alert on withdrawal anomalies: duplicate withdrawal IDs, cooldown failures, max-withdrawable violations, asset rate-limit violations, liquidity failures, and emergency-mode rejections.
- Alert on slot and snapshot integrity: stale or gapped snapshot IDs, unusually long publication gaps, insufficient qualifying slots, duplicate batch indexes, batch-count mismatch, and pending snapshots.
- Document signer rotation: define who approves rotation, how stale keys are revoked, and how signer-rotation events are validated.
- Pre-stage incident scripts for emergency mode, role revocation, withdrawal block, and post-incident reconciliation.

V1 fallback/hotwallet requirements

- Define numeric small-amount thresholds by asset, user, and rolling time window.
- Set hard V1 balance caps for USDC and USDT that reflect fallback demand only.
- Enforce the less-than-3-day maximum fallback eligibility rule as a blocker, not as a default workflow.
- Record every V1 fallback withdrawal with user, asset, amount, deposit time, reason, approval workflow, and post-withdraw reconciliation.
- Alert on AdminChanged, Upgraded, implementation changes, V1 balance-cap breaches, and any V1 outflow not tied to an approved fallback record.

Position layer requirements

- Maintain freshness dashboards for Polygon and XDC lastSyncedTime and syncFrequency.
- Block dependent risk/withdrawal decisions when processedBatches does not equal totalBatches.
- Alert on registerUser, updateUserAddress, registerAsset, updateAssetSymbol, updateAssetScale, setWithdrawEnabled, setWithdrawLockDuration, and setWithdrawAutoReleaseDuration.
- Retain batch payloads and publisher signatures so snapshots can be reconstructed during incident review.

Go-live acceptance item	Pass condition
V5 primary route	All normal funding and withdrawal flows route through V5 unless documented fallback criteria apply.
V1 fallback policy	Numeric small thresholds, less-than-3-day rule, and caps are defined and enforced.
Role custody	Privileged roles are multisig/equivalent and monitored in real time.
Publisher reconciliation	Signed/replayable reconciliation artifacts exist for every published balance batch.
Snapshot freshness	Automated stale/gap/batch alerts are active and tested.
Withdrawal monitoring	Withdrawal ID uniqueness, max withdrawable, rate limits, and liquidity checks are monitored.
Incident readiness	Emergency-mode and role-revocation runbooks are tested.
Audit trail	Every fallback and manual exception has a workflow ID and post-action reconciliation record.

15. Final Opinion

Final status: PASS

No Critical, High, or Medium finding was identified within the public smart-contract, public ABI, public explorer, and deployment-posture scope reviewed. V5 materially improves the primary funding risk posture relative to V1 fallback/hotwallet usage.

The V5 funding architecture is the recommended primary path because the exact-match verified Ethereum FundingContractV5 source and production deployment posture show role-separated publication and withdrawal functions, registration-anchored event-based three-slot cadence, batch integrity checks, cooldown and max-withdrawable checks, duplicate-withdrawal prevention, per-asset rate limits, liquidity checks, emergency mode, signer rotation, and transfer invariants. XDC deployment/activity was reviewed separately, with source verification pending on XDCScan at the review date.

V1 should remain a capped fallback/hotwallet path for narrow cases only: a user deposits and attempts to withdraw a small amount within less than 3 days, the request passes reconciliation and risk checks, V1 cap/liquidity checks pass, and an independent approval workflow records the exception. Any broader use of V1 would weaken the V5 primary-funding risk posture.

The PASS conclusion is therefore conditional on accurate public product descriptions, continued V5-primary routing, formal V1 fallback thresholds, rigorous role/key management, publisher/offline engine controls, and continuous monitoring of snapshots, batches, withdrawals, and proxy/governance events.

A. Appendix A - Source Evidence Matrix

ID	Source	URL	Use in opinion
E1	Existing Quote.Trade public audit PDF	https://quote.trade/docs/quote-trade-audit.pdf	Prior public-scope audit format, scope language, PASS framing, and limitations.
E2	Ethereum V5 funding contract	https://etherscan.io/address/0xe430d7906c3d3144223cf2b4d0d2eb16247d6881	Explorer identifies the address as exact-match verified FundingContractV5 with recent role, registration, and balance-publication activity. Used for V5 deep-review controls, constants, and deployment posture.
E3	XDC V5 funding contract	https://xdcscan.com/address/0xE430d7906c3D3144223cF2b4d0d2eb16247d6881	Explorer identifies the production address and recent role, asset, user-registration, and balance-publication activity. XDCScan did not display verified source at the review date.
E4	Ethereum V1 fallback/hotwallet proxy	https://etherscan.io/address/0x8815e8f0eb65e1072518e8f842c3ad5199dfcef1	Explorer identifies the address as TransparentUpgradeableProxy with proxy tabs and implementation indirection.
E5	Polygon PositionManager	https://polygonscan.com/address/0xf857aC7bed76B43c5457f56483803C4CebbD7eff	Explorer identifies the address as PositionManager with verified source and frequent batchUpdatePositions transactions.
E6	XDC PositionManager	https://xdcscan.com/address/0xf857aC7bed76B43c5457f56483803C4CebbD7eff	Explorer identifies the address as PositionManager with verified source and frequent batchUpdatePositions transactions.
E7	Ethereum V5 USDC holder page	https://etherscan.io/token/0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48?a=0xe430d7906c3d3144223cf2b4d0d2eb16247d6881	Point-in-time token-holder balance and token-transfer context for the Ethereum V5 funding address.
E8	Ethereum V5 USDT holder page	https://etherscan.io/token/0xdac17f958d2ee523a2206206994597c13d831ec7?a=0xe430d7906c3d3144223cf2b4d0d2eb16247d6881	Point-in-time token-holder balance and token-transfer context for the Ethereum V5 funding address.
E9	XDC V5 USDC holder page	https://xdcscan.com/token/0xfa2958cb79b0491cc627c1557f441ef849ca8eb1?a=0xE430d7906c3D3144223cF2b4d0d2eb16247d6881	Point-in-time XDC USDC holder balance and token-transfer context for the XDC V5 funding address.
E10	Ethereum V1 USDC holder page	https://etherscan.io/token/0xa0b86991c6218b36c1d19d4a2e9eb0ce3606eb48?a=0x8815e8f0eb65e1072518e8f842c3ad5199dfcef1	Point-in-time token-holder balance context for the V1 fallback/hotwallet address.
E11	Ethereum V1 USDT holder page	https://etherscan.io/token/0xdac17f958d2ee523a2206206994597c13d831ec7?a=0x8815e8f0eb65e1072518e8f842c3ad5199dfcef1	Point-in-time token-holder balance context for the V1 fallback/hotwallet address.

B. Appendix B - Monitoring and Alert Checklist

Alert category	Trigger examples	Suggested severity
V5 role changes	RoleGranted, RoleRevoked, grant/revoke balance-poster, withdrawal, guardian roles	High
V5 withdrawals	WithdrawalExecuted, duplicate withdrawal attempt, withdrawal cooldown failure, max-withdrawable breach	High
V5 outflow velocity	Hourly/daily asset withdrawal thresholds approaching or exceeded	High
V5 liquidity	InsufficientContractLiquidity or contract balance below policy threshold	High
V5 snapshot integrity	StaleSnapshotId, SnapshotIdGap, BatchCountMismatch, DuplicateBatchIndex, SnapshotUpdatePending, InsufficientSnapshots, unusually long publication gap	High
Emergency state	EmergencyModeActivated, EmergencyModeExpired, guardian action, signer-rotation required	Critical/High
V1 proxy changes	AdminChanged, Upgraded, implementation change, unknown proxy admin activity	Critical
V1 cap breach	USDC/USDT balance or outflow above hotwallet cap; V1 withdrawal without approved exception record	High
Position freshness	lastSyncedTime exceeds syncFrequency or processedBatches != totalBatches	High
Mapping/config changes	registerUser, updateUserAddress, registerAsset, setSupportedAsset, updateAssetScale/symbol	Medium/High

Daily control	Expected evidence
Reconcile V5 contract balances to internal ledger	Daily signed reconciliation file, exception report, and reviewer sign-off.
Check V1 caps	Balance report showing V1 balances below cap and every V1 outflow mapped to an approved exception.
Review stale snapshot dashboard	No open stale/gap/batch incidents or documented approvals for holds.
Review role/config events	No unapproved role, asset, mapping, or emergency events.
Review withdrawal exceptions	All exceptions have workflow IDs and post-withdraw reconciliation.

C. Appendix C - Glossary

Term	Meaning in this report
V5 funding wallet	FundingContractV5 contract treated as the primary funding wallet architecture.
V1 fallback/hotwallet	Upgradeable V1 funding address used only for capped, small, recent deposit-withdraw exception handling.
Publisher	Operational actor or service that publishes reconciled balances/positions to public contracts.
Offline engine	Off-chain reconciliation and risk system used to compute balances, exposure, PnL, and withdrawal eligibility.
PositionManager	Positions-only ledger contract surface used to publish/query position state; not a primary funding wallet.
Snapshot	A structured balance or position publication. V5 qualifies new funding slots by event-based commit cadence rather than consecutive calendar days.
Batch completeness	Condition that all expected batches for a snapshot were received and no duplicate/missing indexes exist.
Non-upgradeable posture	Public explorer/ABI evidence indicates the contract is a direct deployment rather than a V1-style upgradeable proxy.
Residual risk	Risk that remains after design controls and recommendations, usually because it depends on operations outside public code.