



SMART-CONTRACT SECURITY REVIEW · PUBLIC SUMMARY

H10XVault 1.1.0 → 1.3.0

Static analysis, two rounds of manual review with proofs of concept and adversarial testing, the fixes, and verification on the live Hedera testnet.

REVIEW DATES

30 September – 5
October 2026

SCOPE

H10XVault, the contract
that holds the basket

COMPILER

solc 0.8.28 · cancan ·
200 runs · metadata
hash

PROJECT

H10X Index ·
h10xindex.xyz

This is a self-review made by the H10X team before a professional audit. It is not an audit. It records what automated tools and two rounds of manual review found, what was changed, and how the changes were tested. An independent professional audit is planned as the next step.

AUTOMATED TOOLS

0

exploitable issues left
once every Slither and
Aderyn result was
checked by hand

MANUAL REVIEWS

1 + 9

findings: M-1 in 1.1.0,
then 3 Medium and 6
lower in 1.2.0. 1.3.0 fixes
all but two (F-1, F-5)

AUTOMATED TESTS

124 / 124

tests pass; adversarial
campaigns of millions of
random calls found no
violation

LIVE TESTNET

Passed

1.2.0 handled the attack
live; 1.3.0 passed its full
rehearsal, including a
token deleted by its
issuer

In plain terms

- **Two standard analysers** checked the contract; after hand review, nothing exploitable remained.
- **The first review** found one weakness (a tiny donation could block a basket change), fixed in 1.2.0 and proven on the live testnet.
- **A deeper review before mainnet** found edge cases: a token deleted by its issuer could stop issuance forever, a pending exit could be sandwiched, and stale orders could hit the wrong token. **1.3.0 fixes them.**
- **Guaranteed:** nobody, the team included, can create H10X without the basket, take basket tokens out directly, or pause redemptions. **Trusted:** the team multisig, which decides the rebalancing trades (section 8).

Contents

- 1 Scope and method
- 2 Tool results: 1.1.0, 1.2.0 and 1.3.0
- 3 Finding M-1 and the 1.2.0 fix
- 4 Pre-mainnet review and 1.3.0
- 5 Triage of every tool finding
- 6 Automated tests
- 7 Live verification on Hedera testnet
- 8 Trust assumptions and next steps

What was reviewed, and how

ITEM	DETAIL
Contract	H10XVault holds the basket, issues and redeems H10X, and rebalances. The review also covers the interfaces it uses to call the SaucerSwap routers.
Versions	1.1.0 (first review), 1.2.0 (fixes M-1, verified on testnet) and 1.3.0 (fixes from the pre-mainnet review). All run on the Hedera EVM with HTS tokens.
Compiler	solc 0.8.28, EVM <code>cancun</code> , optimizer on (200 runs), metadata hash embedded for exact-match source verification
Runtime size	1.3.0 is 23,882 bytes, 694 bytes under the 24,576-byte limit.
Static analysers	Slither 0.11.6 (102 detectors) and Aderyn 0.6.8 (88 detectors)
Tests	Foundry unit, fuzz and invariant tests, proofs of concept and mutation testing, against simulated HTS and SaucerSwap environments
Live network	Hedera testnet, with real HTS tokens, real SaucerSwap V1 and V2 routers, and a multisig as the rebalancer

Procedure

1. **Slither and Aderyn on 1.1.0.**
2. **Hand triage of every result:** each one was classed as a real issue, a false positive, intentional, accepted or style (section 5).
3. **Manual review** of what automated tools handle poorly: griefing, HTS token behaviour and role boundaries. This step found **M-1**.
4. **Fix in 1.2.0**, with 14 new tests. The 85 existing tests are unchanged and still pass.
5. **Slither and Aderyn again on 1.2.0**, with the new results triaged the same way.
6. **Launch simulator:** the whole mainnet launch, run off-chain against the 1.2.0 rules.
7. **Live testnet rehearsal** of 1.2.0: the attack, the fixed exit, issue and redeem; and of **1.3.0**: the full deployment, issue and redeem, a bounded exit and a token deleted by its issuer (section 7).
8. **Pre-mainnet review in four tracks** (manual with proofs of concept, adversarial testing, Hedera's token service on mainnet, the deployment procedure), then **1.3.0** and a second pass of every track (section 4).

How the vault works

H10X is a native Hedera (HTS) token. The vault contract is its treasury and its only supply key, and the token has no admin key. The vault holds a basket of up to 10 HTS tokens.

- **Issue:** anyone deposits the basket in proportion and receives H10X. Nobody can create H10X any other way.
- **Redeem:** anyone burns H10X and receives their share of every token in the basket. Redemptions can never be paused.
- **Rebalance:** only the rebalancer (the team multisig) can trade, selling one basket token for another through the fixed SaucerSwap routers.
 - Every swap needs a minimum output, measured from the vault's balances. Swaps of a token that stays are capped; a token being removed can be sold in one swap.
 - The rebalancer chooses the route and the minimum, so holders trust it with the basket's value (section 8).
- **Owner (the same multisig):** manages the basket and the fees within hard limits. It cannot create H10X without the basket, take basket tokens out directly, or pause redemptions.

Slither and Aderyn on every version

Severities are the tools' own labels, not confirmed ones. Every result was checked by hand (verdicts explained in section 5).

TOOL	VERSION	DETECTORS	1.1.0	1.2.0	1.3.0
Slither	0.11.6	102	26 • 0 H, 6 M, 17 L, 3 I	31 • 0 H, 10 M, 19 L, 2 I	28 • 0 H, 10 M, 18 L, 0 I
Aderyn	0.6.8	88	11 types • 51 inst.	11 types • 50 inst.	10 types • 50 inst.

Slither 0.11.6, results by detector

DETECTOR	TOOL SEVERITY	1.1.0	1.2.0	1.3.0	VERDICT
<code>incorrect-equality</code>	MEDIUM	1	3	3	Intentional: exact zero checks (T3)
<code>reentrancy-no-eth</code>	MEDIUM	0	2	2	Accepted: it is the M-1 fix itself (T1)
<code>uninitialized-local</code>	MEDIUM	3	3	3	Intentional: these start at zero on purpose (T4)
<code>unused-return</code>	MEDIUM	2	2	2	False positive: balance changes are measured (T5)
<code>reentrancy-benign</code>	LOW	0	2	2	Accepted (T1)
<code>calls-loop</code>	LOW	10	10	10	Accepted: the basket has at most 10 tokens (T7)
<code>missing-zero-check</code>	LOW	6	6	6	Intentional: the zero address disables a role (T6)
<code>reentrancy-events</code>	LOW	1	1	0	The HBAR sweep was removed in 1.3.0 (T8)
<code>costly-loop</code>	INFO	1	0	0	Loop moved to an internal helper; still bounded (T10)
<code>cyclomatic-complexity</code>	INFO	1	1	0	Checks split into helpers in 1.3.0 (T14)
<code>low-level-calls</code>	INFO	1	1	0	The HBAR sweep was removed in 1.3.0 (T8)
Total		26	31	28	0 exploitable

The 5 Slither results added in 1.2.0 come from the M-1 fix: the token is removed after the sale, and two checks test for exactly zero. 1.3.0 adds no new detector type. Dependencies are excluded, as in every run; including them adds reentrancy flags on calls to Hedera's token service in owner-only set-up functions (T15).

Aderyn 0.6.8, issues and instances

ISSUE	TOOL SEVERITY	1.1.0	1.2.0	1.3.0	VERDICT
State change after external call	HIGH	3	2	2	False positive (T2)
Centralization risk	LOW	16	16	15	By design (T13)
Costly operations inside loop	LOW	3	3	3	Accepted, bounded (T10)
Large numeric literal	LOW	1	1	1	Style (T11)
Literal instead of constant	LOW	3	3	6	Style: key-type bit masks (T11)
<code>nonReentrant</code> is not the first modifier	LOW	8	8	8	Accepted (T9)
Loop contains <code>require</code> / <code>revert</code>	LOW	6	6	6	Accepted (T7)
Address variable set without checks	LOW	4	4	4	Intentional (T6)
Contract has TODO comments	LOW	1	1	0	False positive; gone with the English comments (T12)
Unchecked return	LOW	2	2	2	False positive (T5)
Uninitialized local variable	LOW	4	4	3	Intentional (T4)
Total instances		51	50	50	0 exploitable

Replacing a basket token could be blocked with a dust donation

LOW / MEDIUM · AVAILABILITY

FIXED IN 1.2.0

VERIFIED ON TESTNET

The problem in 1.1.0:

- To remove a token from the basket, the owner called `removeComponent`. That only worked if the vault's balance of the token was exactly zero.
- The vault can receive every basket token, so anyone could send it 1 unit right after the last sale. That unit could never be sold, because the per-swap cap of 20% allows 0 units of a balance that small.

Impact: the basket is full (10 of 10 tokens), so an attacker could stop a token from being replaced for as long as they kept doing this. No funds were at risk, and issue and redeem kept working.

1.1.0: exit in two steps

GRIEFABLE

- The rebalancer sells the token in swaps of up to 20%.
-  **Attacker** sends 1 unit to the vault, at almost no cost.
- The owner tries to remove the token. **It fails: the balance is not zero.**
- Selling the last unit **fails too**: the cap allows 0 units.
- The attacker can repeat this after every try, so the token can never be replaced.

1.2.0: exit in one atomic swap

FIXED

- The owner sets the token's target weight to **0**, which means it is leaving the basket.
-  **Attacker** sends 1 unit while the sale waits for signatures.
- The rebalancer sells with `SELL_ALL`. The amount is the balance **when the swap runs**, donation included, and no cap applies.
-  **The balance is 0 and the weight is 0, so the token leaves the basket in the same transaction.** Anything sent after that is ignored.

What changed in 1.2.0

RULE	1.1.0	1.2.0
Per-swap cap for a token whose weight is 0	20% of its balance	No cap. The owner has already decided that the token leaves.
Amount sold	Fixed when the swap is proposed	Can be <code>SELL_ALL</code> : the whole balance, measured when the swap executes
Removing the token	A separate owner transaction that needs a balance of exactly 0	Automatic , in the same transaction as the final sale
Minimum output, overspend and shortfall checks	Required	Unchanged, still required
Tokens with a weight above 0; who can swap	Cap applies; rebalancer only	Unchanged: cap applies, <code>SELL_ALL</code> rejected; rebalancer only

Still true

- Selling all of a token whose weight is above 0 does not remove it. Only a token set to weight 0 leaves the basket.
- Accepted edge case (F-5): dust sent to a token that never held a balance can block its removal; buying some and exiting it works around it. Nothing is at risk.

Refined in 1.3.0

Selling "the whole balance at execution" also sold growth that arrived while the sale awaited signatures, under a minimum computed for less (F-8, section 4). Since 1.3.0 the signed amount is an **upper bound**: the planned amount plus 1%. Dust inside the margin is still sold and the token still leaves at once, so M-1 stays fixed.

A deeper review before an immutable launch, and 1.3.0

The vault cannot be changed once it is on mainnet, so 1.2.0 was reviewed again in four separate tracks: a manual review with proofs of concept, adversarial testing, research on Hedera's token service as it runs on mainnet today, and a review of the deployment procedure. No way for an outsider to take funds from the vault, mint H10X without paying, or block redemptions was found.

ID	SEVERITY	FINDING IN 1.2.0	IN 1.3.0
F-1	MEDIUM	The rebalancer chooses each swap's route and minimum output, so a malicious or compromised multisig could move the basket's value out through pools it controls. The earlier claim that the owner "cannot withdraw basket assets" was too broad.	BY DESIGN The multisig is trusted with the basket's value; the signing page shows every hop and warns about unusual routes and low minimums (section 8).
F-2	MEDIUM	A basket token deleted by its issuer (or paused, frozen) stopped new issuance forever and could never be removed.	FIXED A deleted token can be removed even with a balance, and never re-added. Tokens with pause, freeze or KYC keys are refused.
F-8	MEDIUM	The 1.2.0 exit sold the whole balance at execution under a minimum fixed earlier; growth in between weakened the protection and allowed a well-timed sandwich.	FIXED The amount is an upper bound (planned + 1%).
F-3	LOW	Orders built for one basket order (amounts, minimums, the skip mask, weights) could hit a different token after a removal and an addition.	FIXED A configuration version: stale orders revert.
F-4	LOW	Weights could stop adding up to 100%, and a new token started in "exiting" mode, without the per-swap cap.	FIXED Removal needs weight 0; a token is added together with its weight.
F-6	LOW	A token whose issuer could add transfer fees later could join the basket.	FIXED Fee-schedule keys and custom fees are refused.
F-7	INFO	A fee change between quote and issue gave slightly fewer H10X.	FIXED by the configuration version.
F-5	INFO	Dust can still block removing an empty token (M-1 edge case).	ACCEPTED Workaround documented.
I-2	INFO	An owner function could take the vault's HBAR, which pays the token's auto-renewal.	REMOVED Nothing can take HBAR out of the vault.

What changed in 1.3.0

- **Configuration version.** It changes whenever a token is added or removed or the fees change. Issue, redeem and weight changes carry the version they were prepared for and revert if it moved, so nothing applies to the wrong token.
- **Governance cannot block redemptions.** A holder may redeem with "any version", so configuration changes cannot hold anyone in.
- **Admission rules for basket tokens:** no deleted tokens, no custom fees, and no KYC, freeze, pause or fee-schedule key. The 10 planned mainnet tokens pass, checked live on 5 October 2026.
- **Deleted tokens** can be removed; issuance resumes.
- **Exits** sell up to a signed upper bound.
- **A token is added together with its target weight.**
- **The HBAR sweep was removed.**

Evidence

- **124 repository tests** pass, 24 of them new for 1.3.0, including fuzz tests of the exit bound.
- **Proofs of concept** for every finding were ported to 1.3.0 as regression tests: 141 pass.
- **Adversarial suite:** 153 tests; stateful campaigns of up to 1.25 million random calls and 20,000-step random walks, with no violation of solvency, no free mint, fees, redeem liveness, backing per H10X or stale-order protection.
- **Mutation testing:** 35 of 36 deliberate bugs were caught (the survivor changes nothing).
- **Hedera checks on mainnet:** missing token keys are reported without reverting, as the admission rules require.
- **Slither and Aderyn** report nothing new (section 2).

Every tool finding, checked by hand

#	TOOL • DETECTOR	WHERE	VERDICT	REASON
T1	Slither • reentrancy-no-eth and reentrancy-benign NEW IN 1.2.0	<code>rebalanceV1</code> , <code>rebalanceV2</code> (step after the trade)	Accepted	The fix needs the token to be removed after the sale. Both functions are protected against reentrancy and can only be called by the rebalancer. The routers are fixed SaucerSwap contracts, and basket tokens are HTS tokens, which have no transfer hooks. Every other non-owner function that changes state is also protected against reentrancy, and the router cannot reach the owner functions.
T2	Aderyn H-1 • state change after external call	<code>issue</code> , <code>redeem</code>	False positive	The calls made before the state change are read-only balance queries and HTS transfers, inside functions protected against reentrancy.
T3	Slither • incorrect-equality (×3)	<code>burnStrayShares</code> , trade checks	Intentional	These are exact zero checks. Some skip work when there is nothing to do. The other is "balance is exactly 0", which is the condition for removing a token. The balance cannot change between the swap and the check, which run in the same transaction; a donation made earlier, within the signed bound, is sold with the rest.
T4	Slither • uninitialized-local / Aderyn L-10	<code>issue</code> , <code>initialize</code> , weight setting	Intentional	These variables are meant to start at zero.
T5	Slither • unused-return / Aderyn L-9	<code>rebalanceV1</code> , <code>rebalanceV2</code>	False positive	The amount received is measured from the vault's balance changes, which is stricter than trusting the router's return value.
T6	Slither • missing-zero-check / Aderyn L-7	constructor, <code>setGuardian</code> , <code>setRebalancer</code>	Intentional	Setting the zero address disables a router, the guardian or the rebalancer. The fee recipient is checked.
T7	Slither • calls-loop / Aderyn L-6	<code>issue</code> , <code>redeem</code> , quotes, <code>seed</code>	Accepted	The loops run over at most 10 tokens. If one token starts failing, <code>issue</code> fails safely, and <code>redeem</code> can skip that token so holders still get everything else.
T8	Slither • reentrancy-events, low-level-calls	<code>sweepHbar</code>	Removed	Owner-only HBAR sweep in 1.1.0 and 1.2.0; removed in 1.3.0 (I-2).
T9	Aderyn L-5 • <code>nonReentrant</code> is not the first modifier	8 functions	Accepted	The modifiers that run before it make no external calls.
T10	Aderyn L-2 / Slither costly-loop	removing a token, basket set-up, weight setting	Accepted	At most 10 iterations.
T11	Aderyn L-3, L-4	numeric literals	Style	A literal value is clearer here.
T12	Aderyn L-8 • TODO comments	a comment	False positive	It matched the Spanish word "todos" ("all").
T13	Aderyn L-1 • centralization	owner functions	By design	The owner's powers and limits are listed in section 8.
T14	Slither • cyclomatic-complexity	token-adoption check	Accepted	It is a straight list of on-chain checks (split into helpers in 1.3.0).
T15	Slither with dependencies • reentrancy	set-up, adding and removing tokens	False positive	The "external call" is a query to Hedera's token service, which never calls back into the vault. These functions are owner-only, and HTS tokens have no transfer hooks.

124 tests, adversarial campaigns, a launch simulator and the size limit

TEST SUITE	TESTS	WHAT IT COVERS
Core behaviour	53	Issue, redeem, fees, roles, pauses, basket management and removal rules, rebalancing on V1 and V2, limits and error cases
Token adoption	21	The vault takes control of the H10X token only if it is the treasury and the only supply key, the token has no forbidden keys or custom fees, and its settings are correct. Combinations of keys are fuzzed.
Economics and attacks	9	Arbitrage around NAV, a whale, an attacker, a sandwich attack, and the ± 81 bp price band
Invariants	3	Backing per H10X never decreases: 128 runs of 40 random calls each (issue, redeem, fee claim, donation and burn), with no reverts
Finding M-1 (1.2.0)	14	The exit flow (listed below)
Pre-mainnet fixes (1.3.0)	24	New: configuration version and stale orders, the redeem "any version" option, the exit bound (including fuzz tests), admission rules, adding a token with its weight, removing a deleted token
Total	124	124 passed • 0 failed • 0 skipped

The 14 tests for M-1 (1.2.0)

- The contract reports its version, and `SELL_ALL` is the maximum value.
- **A donation made before the sale is sold with the rest, and the token leaves the basket in the same transaction.** This is tested on both router versions, and the router permissions go back to zero.
- A donation after removal is harmless: issue and redeem keep working with the remaining tokens.
- A token with weight 0 ignores the 20% cap. A partial sale keeps it in the basket.
- Selling the exact full balance also removes the token.
- With a weight above 0, `SELL_ALL` and oversized sales are rejected.
- With a weight above 0, emptying the token does *not* remove it.
- A minimum output of 0 is rejected.
- If the pool pays less than the minimum, the whole swap reverts, and nothing is sold or removed.
- Once the token is removed, it can no longer be traded.
- Only the rebalancer can sell. The owner cannot.
- The owner's direct removal still requires a zero balance.
- **Fuzz test:** for any donation from 0 to 10^{15} units, everything is sold and the token is removed.

Contract size (EIP-170 limit)



Launch simulator

An off-chain simulator of the whole mainnet launch follows the 1.3.0 rules and runs end to end without errors: the multisig, the deployment and its checks, the handover, the seed and the Founders Pass airdrop, weight changes, a bounded exit, a stale proposal that reverts as intended, a token deleted by its issuer, and an interruption at every deployment step (running the same command again never creates a second contract or token).

Hedera testnet: 1.2.0 on 30 September, 1.3.0 on 5 October 2026

We ran the attack in its hardest form. The 1 unit arrived **after** the sale had been proposed to the multisig and **before** the sale executed. A fixed sale amount would have left that unit behind. Every ID below can be checked on HashScan.

ENVIRONMENT	ID ON HEDERA TESTNET
Vault, H10XVault 1.2.0 (no admin key)	0.0.10793965
H10X test token (the vault is treasury and only supply key)	0.0.10793966
Owner account, which pays the transactions	0.0.10754475
Rebalancer and guardian: a test multisig needing 2 of 3 signatures	0.0.10762876
Basket	10 test tokens priced at real mainnet prices, traded on the SaucerSwap V1 and V2 testnet routers
Deployment	A new 1.2.0 deployment with its own H10X token. All 8 post-deployment checks passed.

Sequence (UTC)

#	STEP	TRANSACTION	RESULT
1	Seed: 100 H10X at the reference index NAV of \$1.089155	0.0.10754475@1790781057.462333312 15:10:57	SUCCESS
2	tGRELf target weight set from 5% to 0%; the other weights rise pro rata (tWHBAR 20% → 21.1%, ...)	0.0.10754475@1790781119.514665048 15:11:59	SUCCESS
3	Sale proposed to the multisig as a scheduled transaction: tGRELf → tWHBAR, amount <code>SELL_ALL</code> , minimum 50.363351 tWHBAR	schedule 0.0.10794087	PENDING
4	Attack: 1 minimal unit of tGRELf sent to the vault. Vault balance: 4,966,004,353 → 4,966,004,354 units	0.0.10754475@1790781134.128294717 15:12:14	SUCCESS
5	Two members sign and the sale executes. Everything is sold, and tGRELf leaves the basket in the same transaction.	schedule 0.0.10794087	SUCCESS · 2/2
6	Regression: issue 1 H10X (0.995 received after the 0.5% fee)	0.0.10754475@1790781185.132990545 15:13:05	SUCCESS
7	Regression: redeem 1 H10X (a share of all 9 remaining tokens)	0.0.10754475@1790781197.832873620 15:13:17	SUCCESS

To check a transaction, search its ID on hashscan.io/testnet.

What the vault showed

	BEFORE THE EXIT	AFTER THE SALE
Tokens in the basket	10	9
tGRELf	weight 0% · 49.66004354 (seed plus the donated unit)	no longer in the basket
tWHBAR balance	201.51	252.12 (+50.61)

	BEFORE THE EXIT	AFTER THE SALE
Swap	quote 50.616434 • minimum 50.363351	≈ 50.61 received, 0.47% below the reference price
NAV per H10X	\$1.089155 (seed)	\$1.090959
Target weights	100% in total, tGRELf at 0	100% in total across 9 tokens

After issuing and then redeeming 1 H10X, supply was 100.005 H10X, fees accrued were 0.01 H10X (0.5% in plus 0.5% out), and NAV was \$1.102351.

The token's keys did not change:

- the vault is still the only supply key;
- the only other key is the metadata key, which is used for the logo and cannot create, freeze or move tokens;
- the contract has no admin key, so it cannot be changed.

Result: M-1 is fixed on a live network.

A donation made while the sale was pending did not block the exit. The swap sold everything, donation included, and the token left the basket in the same transaction. Issue, redeem and fees work as before.

1.3.0 rehearsal, 5 October 2026

The same deployment as on mainnet, with the test multisig as guardian and rebalancer. The vault [0.0.10872949](#) has no admin key and its source is verified on Sourcify with an **exact match**; its H10X test token is [0.0.10872951](#).

#	STEP	RESULT
1	Deployment, then the setup of the 10 tokens in one transaction	HEDERA LIMIT nothing changed
2	Setup in two steps: 5 tokens, then the other 5 added one by one. Same final basket and weights; all 11 post-deployment checks pass	SUCCESS
3	Seed of 20 H10X, issue 1, redeem 1, and redeem 0.5 with the "any version" option	SUCCESS
4	Exit of tGRELf: the sale is proposed to the multisig with a signed upper bound; 2 of 3 members sign; everything is sold and tGRELf leaves the basket in the same transaction	SUCCESS • 2/2
5	A basket token is deleted by its issuer (test token tDEL, 1% of the basket, with 1,000 tDEL in the vault)	Transfers of tDEL now fail
6	Redeem 1 H10X giving up tDEL: the holder receives the other 9 tokens	SUCCESS
7	tDEL removed from the basket although the vault still holds 1,000 tDEL : the vault asks Hedera's token service and sees that it is deleted	SUCCESS
8	Issue 1 H10X: issuance works again (in 1.2.0 it would have stopped for good)	SUCCESS
9	Adding tDEL back, sent straight to the contract	REJECTED ComponentDeleted

A Hedera limit, measured. Hedera allows at most 50 "child records" per transaction, and every call from the vault to the token service creates one, read-only queries included. Setting up 10 tokens at once needs 68, so the deployment now does it in two steps; the contract is unchanged. Everyday operations stay within the limit with the maximum of 10 tokens: issue needs 43, the seed 33 and redeem 25, counted on the live transactions above.

Result: 1.3.0 behaves as designed on a live network.

Issue and redeem with the configuration check, the bounded exit, the redeem escape hatch and the removal of a deleted token all work on Hedera's real token service. The two problems found during the rehearsal were in the deployment and monitoring tools (the transaction limit above, and how the public mirror node reports a deleted token), not in the contract; both are fixed in the tools that will be used on mainnet.

What holders and auditors should know

1. **The multisig is trusted with the basket's value (F-1).** On mainnet the owner and the rebalancer are a team multisig that needs several signatures. The rebalancer chooses each swap's route and minimum output; the contract has no on-chain price limit and no cooldown.
 - A malicious or compromised multisig could therefore move value out of the basket through swaps against pools it controls. While weights are unchanged this is limited to the per-swap cap of each token; the owner can raise the cap or set a weight to 0, which removes it.
 - Every governance action is a scheduled transaction that the members sign on the project's signing page. The page decodes the call from Hedera itself, shows every hop of a route with its fee tier, and warns about tokens outside the basket, minimum outputs far below the current price, and proposals made for an old configuration. Members are asked to cross-check on HashScan.
 - Possible hardening, to discuss with the auditor: an on-chain price bound (time-weighted price), a cumulative limit per period, and a timelock.
2. **The owner can:**
 - add tokens that pass the admission rules, and remove tokens with weight 0 and no balance (or deleted by their issuer);
 - set target weights, including 0 to remove a token;
 - set fees, up to a hard cap of 1%;
 - set the per-swap cap, the supply cap and the issuance pause.
3. **The owner cannot:** create H10X without the basket, take basket tokens or HBAR out directly, pause redemptions, or give up ownership. A governance change can make a pending redemption revert, but the holder can always redeem with the "any version" option.
4. **Keys on basket tokens.** Basket tokens may not have KYC, freeze, pause or fee-schedule keys. Admin, wipe and supply keys are allowed: an issuer with an admin key could delete its token (it can then be removed from the basket, and its balance is lost), and the bridge contracts behind the wrapped BTC and ETH tokens control their supply. Until a deleted token is removed, redeem can skip it so holders still receive everything else.
5. **No price oracle.** Issue and redeem are strictly proportional, and rounding favours the vault. The invariant tests check that backing per H10X never decreases.
6. **The H10X token.** Before taking control, the vault checks on-chain that it is the token's treasury and only supply key, with no forbidden keys or custom fees (confirmed on testnet).

Status and next steps

- **Deployed on mainnet on 6 October 2026**, the same way as the 1.3.0 rehearsal: vault [0.0.10907483](#) (no admin key; source verified on Sourcify with an **exact match**) and H10X token [0.0.10907484](#). The team's 2-of-3 multisig [0.0.10907480](#) is owner, guardian and rebalancer: it accepted ownership about a minute after the first deposit (the seed), and the deployment account has no role.
- **Public source verification:** done on mainnet. Anyone can read the vault's source code on HashScan or Sourcify and confirm that it matches the code running on-chain.
- **An independent professional audit** of H10XVault 1.3.0, starting from this review. The raw tool output and the test suites are available to auditors on request.

Revision history: 30 Sep 2026, first edition (1.1.0 → 1.2.0). 4 Oct 2026, code comments in English and metadata hash embedded, with identical executable code. 5 Oct 2026, pre-mainnet review and 1.3.0; the trust assumptions were corrected (F-1); results of the 1.3.0 testnet rehearsal. 6 Oct 2026, mainnet deployment, seed and handover to the multisig.