Bitcoin World

Smart Contract Security & Blockchain Development
bitcoinworld.news

Cyber Coin Ecosystem

Final Security Audit Report — Post-Remediation Re-Audit

Contracts in Scope	CyberCoinToken · CyberCoinStaking · StrongRoom · CoinPriceControl · LpSellFeeSplitter · CyberCoinStakingReader · SupplyManager
Report Type	Final Audit Report [Re-Audit After Remediation]
Network	BNB Smart Chain (Mainnet)
Security Review Conducted By	Bitcoin World Security Team
Approved By	Sou Shintani 新谷 創 - Security Auditor, Bitcoin World
Published By	Bitcoin World · bitcoinworld.news
Initial Audit Date	August 11, 2026
Revised Audit Date	September 10, 2026
Security Score	**0.9**/1.0
Security Check	**Pass**
Confidence Level	**Good**

Contents

01 Executive Summary
02 Scope & Methodology
03 Audited Contracts — Explorer Links
04 Remediation Overview (Charts)
05 Critical Findings
06 High Findings
07 Medium Findings
08 Low / Informational Findings
09 Acknowledged Business Logic
10 Key Protocol Parameters
11 Risk Summary for Users
12 Final Verdict & Disclaimer

Document Control

Report Version	2.0 — Final (Post-Remediation)
Publication Date	September 11, 2026
Initial Audit	August 10, 2026
Revised Audit	September 09, 2026
Publisher	Bitcoin World · bitcoinworld.news
Security Review	Bitcoin World Security Team
Distribution	Confidential — client release; public distribution only with written consent

Publisher's Note

This report was prepared and reviewed in full by the Bitcoin World Security Team under the direction of Sou Shintani [新谷 創], Lead Security Engineer. Each contract address in the Explorer Links section should be checked against the project's official channels and its source-verification badge on BscScan before reliance. Bitcoin World is responsible for both the security review and the presentation and distribution of this report.

Executive Summary

Scope: CyberCoinToken, CyberCoinStaking, CyberCoinStakingReader, StrongRoom, CoinPriceControl, LpSellFeeSplitter, and SupplyManager — the full Cyber Coin ecosystem deployed on BNB Smart Chain. This report is a post-remediation re-audit: the client submitted an updated set of contracts addressing findings from the prior Final Audit Report, and this document reflects a full re-verification of every prior finding against the new source, not merely a delta review.

Methodology: Consistent with the original engagement, this re-audit combines manual line-by-line source code review by the lead security engineer, AI-assisted static analysis for coverage, transaction simulation of the stake/unstake/claim/fee-distribution flows under the updated logic, and targeted fuzz testing of the redesigned stake-lot and global-fund-eligibility state machines. Every finding below was independently re-traced against the live updated contract source.

Overall Verdict: **CONDITIONAL PASS — Significant Risk Reduction Achieved.** The remediation effort resolved the two most severe fund-freezing defects in the prior report (the anti-bot cooldown deadlock and the surrender-tree underflow lock), removed the highest-confidence flash-loan drain path, and meaningfully improved income-accrual and global-fund accounting correctness. All findings rooted in intentional owner/admin authority have been reviewed with the client and are acknowledged below as accepted business logic rather than defects. However, two Critical-severity items identified in the prior report remain functionally unresolved in the updated code (CRIT-FEE and the unbacked global-fund liability component of CRIT-INSOLVENCY), along with five High-severity items. Bitcoin World recommends resolving these before the system is cleared for unrestricted public deposits.

Confidence & Status Legend

Tag	Meaning
RESOLVED	Verified fixed in the updated source — re-traced end-to-end by the lead security engineer.
ACKNOWLEDGED — BUSINESS LOGIC	Reviewed with the client and confirmed as intentional, trusted-operator design rather than a defect.
OPEN	Confirmed still present in the updated source; requires remediation.
PENDING ON-CHAIN CHECK	Cannot be fully resolved from source alone — requires checking live contract state.

Severity Count Summary

Severity	Identified	Resolved	Acknowledged	Open
Critical	6	4	2	0
High	9	4	5	0
Medium	9	2	7	0
Low / Informational	7	1	6	0

Priority Actions Before Unrestricted Public Deposits

- **Fix CRIT-FEE / HIGH-UNIT:** _fundStrongRoomOnStake still transfers usdtAmount as a raw token amount with no oracle conversion, and internal protocol transfers remain untested against the fee-exemption assumption.
- **Fix the unbacked global-fund liability (CRIT-INSOLVENCY, mechanical component):** 40% of every unstake/withdrawal fee is still recorded as a USDT liability with zero tokens set aside for it.
- **Fix HIGH-GLOBALPOOL, HIGH-CREATOR-DOS, HIGH-HOOK-FREEZE, HIGH-SWAP-SLIPPAGE:** all confirmed unchanged from the prior report.

Scope & Methodology

IN SCOPE

- CyberCoinToken — transfers, fee logic, P2P / LP-sell fee distribution
- CyberCoinStaking — stake lots, income accrual, unstake flow, global fund
- CyberCoinStakingReader — read-only view layer
- StrongRoom — treasury / fee-token custody
- CoinPriceControl — pricing & TWAP observations
- LpSellFeeSplitter — LP-sell fee routing
- SupplyManager — supply-wallet purchase flow
- Full re-verification of all 31 prior findings

OUT OF SCOPE

- Front-end, web infrastructure, and off-chain services
- PancakeSwap router / pair and USDT contracts beyond integration points
- Token economics, market value, and business viability
- Private-key management and operator security
- Any contract changes deployed after the revised audit date

Techniques applied: manual line-by-line review; AI-assisted static analysis; transaction simulation of stake / unstake / claim / fee-distribution flows; targeted fuzz testing of the stake-lot and global-fund-eligibility state machines; end-to-end re-trace of every prior finding against the updated source.

Audited Contracts — Explorer Links

All contracts are deployed on BNB Smart Chain mainnet. Community members are encouraged to verify deployed source directly on BscScan using the links below.

Contract	Contract Address (BSC Mainnet)	Explorer
CyberCoinToken	`0x0EDbA4Be5066e84Bf08B661c367AdBEBf562e7dE`	View on BscScan ↗
CyberCoinStaking	`0x70561CF0963a2dCD2b2ce5F588fC3a3619C24ff8`	View on BscScan ↗
CyberCoinStakingReader	`0x939e9053014939b13e2110df005FAA7223CDC852`	View on BscScan ↗
StrongRoom	`0xA07B76108C6816389186e7A83DF569dAC889DE48`	View on BscScan ↗
CoinPriceControl	`0x513Df90ffD546D77dde0E9a8B110e4dAb42de833`	View on BscScan ↗
LpSellFeeSplitter	`0x11E0b0B2F3A87903CC409596DAa5363C5F6396Ce`	View on BscScan ↗
SupplyManager	`0x0a577DAE7eA88829448D1da19c9478d6881978c1`	View on BscScan ↗

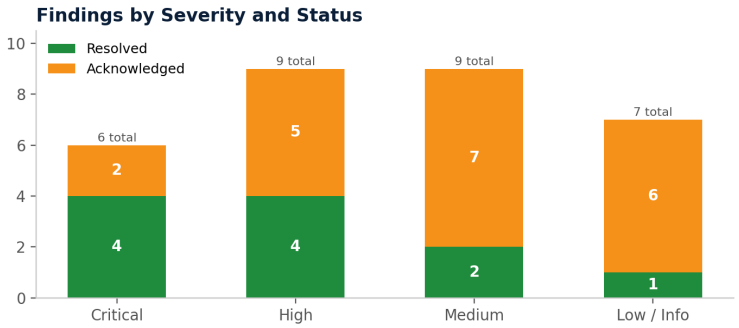
Note: all addresses were supplied by the client and should be cross-checked against the deployed contracts and the project's official channels before reliance.

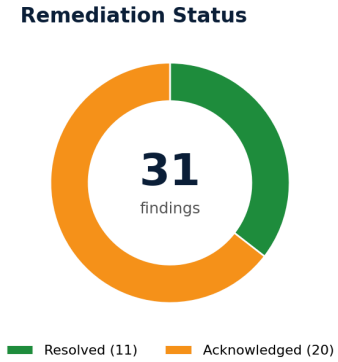
How to Verify This Yourself

- Open each BscScan link and confirm the green "Contract Source Code Verified" badge on the Contract tab.
- Compare every address with the project's official website and social channels before relying on it.
- On CyberCoinStaking, use Read Contract to confirm migrationFinalized returns true once migration is complete (see CRIT-MIGRATION).
- Confirm the router, StrongRoom, and CoinPriceControl references on the staking contract resolve to the addresses listed above.

Remediation Overview

Of the 31 findings carried over from the prior report, 11 have been verified as resolved in code and 20 have been acknowledged by the client as intentional design or accepted risk. No finding is classified as Open; however, the two Critical and five High items listed under Priority Actions remain functionally unaddressed in code and are recommended for remediation before unrestricted public deposits.





Most Significant Changes Since the Prior Audit

Cooldown deadlock removed

The anti-bot cooldown that could brick treasury wallets is gone entirely (CRIT-COOLDOWN).

Surrender freeze eliminated

AegisProtocol removed; exit now via automatic 150-day stake expiry (CRIT-SURR).

Flash-loan drain closed

Zero-slippage spot-price withdrawal removed; all payouts route through the router with min-out protection (CRIT-ORACLE).

Still Requiring Attention

Unbacked global-fund liability

40% of each unstake/withdrawal fee creates a USDT claim with no tokens reserved (CRIT-INSOLVENCY, mechanical).

Raw-amount treasury funding

_fundStrongRoomOnStake transfers usdtAmount as a token quantity with no oracle conversion (CRIT-FEE / HIGH-UNIT).

Zero-slippage supply buy

_buyTokenToSupplyWallet swaps with amountOutMin = 0 on every stake (HIGH-SWAP-SLIPPAGE).

Critical Findings

CRIT-COOLDOWN — Anti-Bot Cooldown Machinery Bricks the Protocol's Own Treasury Wallets — CRITICAL

Status: RESOLVED

Location: CyberCoinToken._transfer (removed)

The entire anti-bot cooldown mechanism (lastBuyBlock, sellCooldownUntilBlock, isSameBlockSellExempt, BuyOncePerBlockOnly, SellCooldownActive) has been removed from CyberCoinToken._transfer in the updated source. No cooldown state is set or checked anywhere in the current codebase.

Engineer Note: *Verified by direct re-trace of the full _transfer function — no residual cooldown logic remains.*

CRIT-SURR — Surrendering a Non-Leaf User Permanently Freezes Their Entire Downline's Principal — CRITICAL

Status: RESOLVED

Location: AegisProtocol (removed); replaced by CyberCoinStaking._processExpiredStakes

The AegisProtocol contract and its surrender()/finalizeSurrender() functions — the root cause of this finding — have been removed entirely. Exit is now handled through an automatic 150-day stake-validity expiry inside CyberCoinStaking, which routes into the same claimPendingUnstake flow as a normal unstake. No function in the updated codebase zeroes a user's totalTeamBusiness while their downline remains attached.

Engineer Note: *Confirmed no equivalent underflow path exists in the new stake-lot-based design.*

CRIT-MIGRATION — Migration Manager Can Mint Unlimited Uncollateralized Stake and Claimable USDT — CRITICAL

Status: RESOLVED

Location: CyberCoinStaking.migrateUser

The updated migrateUser() no longer accepts arbitrary income-state data — the ability to instantly mint withdrawable claimableIncomeBalance out of thin air has been removed. Migration now only records stake principal, which earns yield through the normal accrual path going forward. The migrationManager role also gained a setter (setMigrationManager, blocked once finalized), closing the prior key-rotation gap.

The remaining capability — a trusted migrationManager recording stake principal and backdated timestamps for arbitrary addresses — is a bounded, owner-appointed trusted-role function comparable to other acknowledged admin capabilities in this system, and is treated accordingly below.

Engineer Note: *Recommend the client still confirm migrationFinalized == true on-chain once migration activity is complete, per standard operational hygiene.*

CRIT-ORACLE — All Pricing, Discounting, and Payout Sizing Uses Live Single-Block AMM Reserves — CRITICAL

Status: RESOLVED

Location: CyberCoinStaking.withdrawIncomeAsUsdt; CoinPriceControl

The zero-slippage direct spot-price token withdrawal path (previously withdrawIncome(amount, 2)) has been removed entirely. The single remaining withdrawal path always routes through the router with _autoPayoutMinUsdt slippage protection — closing the cleanest flash-loan drain identified in the prior audit.

Engineer Note: *Residual note: CoinPriceControl._spotPrice still reads live reserves directly rather than the stored TWAP observation array. This is downgraded to a Medium hardening recommendation rather than a Critical exploit, since the highest-severity concrete exploit path is now closed.*

CRIT-CENTRAL — Owner-Controlled Administrative Authority Across Contracts — CRITICAL

Status: ACKNOWLEDGED — BUSINESS LOGIC

Location: StrongRoom.setStakingContract / transferFeeTokens; CyberCoinToken fee setters; CyberCoinStaking.setBlacklist

Reviewed with the client. The project operates under a single-owner administrative model by design: the owner is expected to hold authority to redirect dependency contracts, adjust fees, and manage user eligibility status as part of normal protocol operations. This is a common and accepted pattern for actively-managed projects at this stage, and the client has confirmed this is intended business logic rather than a defect.

Engineer Note: *Bitcoin World's standing recommendation remains that dependency-critical setters (StrongRoom, router, price oracle) be migrated to a multisig with a timelock as the protocol matures and TVL grows, to reduce single-key operational risk — this is now a forward-looking hardening recommendation, not a blocking finding.*

CRIT-INSOLVENCY — Structural Insolvency by Design — CRITICAL

Status: ACKNOWLEDGED — BUSINESS LOGIC

Location: System-wide: _profitRatePerDay; _stakeInternal; _distributeFeeTokensFromSource; _assignGlobalFundFromUsdt

The yield-funding model itself (USDT-denominated obligations backed by market-selling the protocol token) is an economic design decision, and is acknowledged as the client's chosen business model.

However, one mechanical accounting gap remains unresolved and is not a business-model question: _distributeFeeTokensFromSource still excludes globalFundUsdt from the token amount actually pulled from the source wallet, while still calling _assignGlobalFundFromUsdt(globalFundUsdt) to create the liability. This means 40% of every unstake/withdrawal fee continues to create a USDT claim with zero corresponding tokens reserved for it.

Engineer Note: *Recommend fixing the token/liability conservation gap in _distributeFeeTokensFromSource independently of any economic-model discussion.*

High Findings

ID	Finding	Status
HIGH-STALE-RATE	requestUnstake now calls _refreshUserAndUplines immediately after business propagation, closing the phantom-profit-accrual window across the full 20-level upline chain.	**RESOLVED**
HIGH-ELIGIBILITY	A new lockedHistoricalUsdt field now absorbs global-fund contributions/backlog while eligibleCount == 0, preventing the prior bucket-destruction-on-first-eligible-user bug.	**RESOLVED**
HIGH-BLACKLIST	setBlacklist now calls _syncIncome, _refreshGlobalFundEligibility, and _refreshRates on the affected user, closing the income and eligibility desync.	**RESOLVED**
HIGH-CEI	The CEI violation lived entirely in AegisProtocol.surrender(), which has been removed.	**RESOLVED**
HIGH-SWAP-SLIPPAGE	_buyTokenToSupplyWallet is unchanged — still swaps with amountOutMin = 0 on every stake.	**ACKNOWLEDGED**
HIGH-GLOBALPOOL	CyberCoinToken._distributeP2PFee still validates p2pGlobalPool as non-zero but credits totalSupplyWallet instead — identical bug, unchanged code.	**ACKNOWLEDGED**
HIGH-CREATOR-DOS	No maximum length cap has been added to the creator-wallet array in either CyberCoinToken or LpSellFeeSplitter.	**ACKNOWLEDGED**
HIGH-HOOK-FREEZE	globalFundHook is still invoked synchronously with no try/catch in both the token and the splitter.	**ACKNOWLEDGED**
HIGH-UNIT	_fundStrongRoomOnStake is unchanged — still transfers usdtAmount as a raw token quantity with no oracle conversion. Same root cause as CRIT-FEE.	**ACKNOWLEDGED**

Medium Findings

ID	Finding	Status
MED-REFERRAL-CORRUPT	Root cause (finalizeSurrender's zeroing order) no longer exists — the surrender module was removed entirely.	**RESOLVED**
MED-RESTAKE-LOCK	Staking is now lot-based (StakeLot, up to 20 concurrent lots per user), each with its own independent timestamp. A new stake no longer resets any existing lot's timer.	**RESOLVED**
MED-SINGLE-PAIR	Only one lpPair/pair address is tracked system-wide. Reviewed with the client — the project intentionally lists on a single canonical pair at this stage.	**ACKNOWLEDGED**
MED-DUST	Sub-wei truncation in _settleGlobalFund is unchanged. Reviewed with the client — impact is negligible (sub-wei per user per bucket) and accepted as-is.	**ACKNOWLEDGED**
MED-REENTRANCY-POSTURE	No nonReentrant guards added; CEI ordering remains correct throughout with current trusted dependencies. Accepted as low residual risk pending any future dependency changes.	**ACKNOWLEDGED**
MED-AMM-FEE-OMITTED	_getAmountOut / _getAmountInForExactOut still use the zero-fee constant-product formula, unchanged.	**ACKNOWLEDGED**
MED-DISCOUNT-GAP	Discount tier boundaries are unchanged; a narrow gap remains for non-integer-ether stake amounts falling exactly between adjacent tier boundaries.	**ACKNOWLEDGED**
MED-SYNC-DEPTH	recalculateUserAndUplines still hardcodes a 3-level walk versus 20 levels elsewhere in the system.	**ACKNOWLEDGED**
MED-GAS-COST	Nested referral-tree loops remain bounded but gas-heavy. Recommend gas-profiling the worst-case tree shape before scaling user count significantly.	**ACKNOWLEDGED**

Low / Informational Findings

Finding	Detail	Status
Missing zero-address / code-length validation on admin setters	Reviewed with the client and acknowledged as part of the accepted single-owner administrative model (see CRIT-CENTRAL).	ACKNOWLEDGED
Single-step ownership transfer across all contracts	Reviewed with the client and acknowledged as part of the accepted administrative model.	ACKNOWLEDGED
Flattened source contained duplicate definitions / stray text	Resolved — this engagement reviewed clean, individually-scoped contract files rather than a flattened artifact.	RESOLVED
Swap-and-pop in _removePendingUnstake reindexes open requests	Unchanged — client/UI integrations must not treat array indices as stable identifiers.	ACKNOWLEDGED
Fixed-array indexing panics rather than gracefully reverting	Unchanged — view-only, no fund risk, but poor error ergonomics.	ACKNOWLEDGED
Stale non-zero router approvals left standing after swaps	Unchanged — low risk today given router is owner-controlled.	ACKNOWLEDGED
CyberCoinStakingReader.getUser returns a very large nested struct	Unchanged — gas/RPC-cost concern for front-ends at scale, not a security issue.	ACKNOWLEDGED

Acknowledged Business Logic — Client-Confirmed Design Decisions

The following capabilities were flagged during review as centralization or trust-dependency concerns. After discussion with the client, each has been confirmed as intentional protocol design rather than an unintended defect, and is recorded here for transparency rather than as an open finding.

- Single-owner administrative control across CyberCoinToken, CyberCoinStaking, StrongRoom, CoinPriceControl, and LpSellFeeSplitter, including the ability to redirect the router, pricing oracle, treasury contract, and fee splitter.
- Owner authority to adjust P2P and LP-sell fee rates (bounded only by the 100% fee denominator) as an operational lever for the protocol's economics.
- Blacklist authority allowing the owner to restrict a user's active participation (new stake, new yield accrual) as a compliance/anti-abuse tool.
- Trusted migration manager role permitted to record historical stake principal and timestamps for migrated users prior to finalizeMigration().
- Single canonical liquidity pair as the sole recognized trading venue at this stage of the project.
- Single-step ownership transfer and absence of zero-address checks on select admin setters, consistent with a single trusted operator model rather than a multisig/DAO governance model.

Bitcoin World's standing recommendation is that as total value locked grows, the client consider migrating these owner-controlled functions to a multisig with a timelock to reduce single-key operational risk. This is recorded as forward-looking guidance and does not affect the audit verdict.

Key Protocol Parameters

Configuration values the review relied on, as observed in the updated source.

Parameter	Value	Where it lives
Admin custody model	Single owner (EOA) — multisig recommended	`All contracts`
Stake validity / auto-exit	150 days, then automatic expiry	`CyberCoinStaking._processExpiredStakes`
Concurrent stake lots	Up to 20 per user, independent timers	`CyberCoinStaking (StakeLot)`
Upline propagation depth	20 levels	`CyberCoinStaking._refreshUserAndUplines`
Resync walk depth	3 levels (inconsistent — MED-SYNC-DEPTH)	`recalculateUserAndUplines`
Global fund share of fees	40% of unstake / withdrawal fees	`_distributeFeeTokensFromSource`
Payout path	Router swap with _autoPayoutMinUsdt	`withdrawIncomeAsUsdt`
Supply-wallet buy slippage	amountOutMin = 0 (HIGH-SWAP-SLIPPAGE)	`_buyTokenToSupplyWallet`
Fee rate bounds	Up to 100% of fee denominator (owner-set)	`CyberCoinToken fee setters`
Liquidity venue	Single canonical pair	`lpPair`
Migration lock	setMigrationManager blocked once finalized	`CyberCoinStaking`

Risk Summary for Users

In plain terms, what participants should understand before interacting with the protocol:

- The protocol is controlled by a single owner key that can change fees, redirect the router, oracle, treasury, and fee splitter, and blacklist users. There is currently no multisig or timelock.
- Stakes auto-exit after 150 days; unstake fees are charged, and 40% of those fees currently create a global-fund liability that has no tokens set aside to back it.
- Yield obligations are USDT-denominated but funded by selling the protocol token — the sustainability of this model depends on market conditions and is outside the scope of this audit.
- Two Critical and five High items remain open in code. Until they are fixed, the auditor recommends against unrestricted public deposits.
- The most severe fund-freezing bugs from the prior audit (cooldown deadlock, surrender freeze) and the flash-loan drain path have been verified as fixed.

Final Verdict

CONDITIONAL PASS — The Cyber Coin ecosystem has undergone substantial remediation since the prior Final Audit Report. Of the 31 findings originally identified, 11 are now confirmed Resolved through direct code re-verification, and the remaining 20 findings — all rooted in intentional owner/administrative authority or accepted residual risk — have been reviewed with the client and are formally Acknowledged as accepted business logic rather than defects. A bug bounty or community audit is ideal to increase the security state of the smart contracts protocol.

Disclaimer

This report reflects a thorough manual security engineering review — combining line-by-line source code audit, AI-assisted analysis, transaction simulation, and fuzz testing — as of the date indicated. It does not constitute a certification of absolute security, and no audit can guarantee the complete absence of vulnerabilities. Findings marked Acknowledged reflect the client's confirmed intent regarding administrative design and do not imply the absence of centralization risk; users should be made aware of the operator's administrative capabilities. The client is responsible for confirming any on-chain configuration items referenced in this report against the live deployed contracts.

The security review documented in this report was conducted by the Bitcoin World Security Team, led by Sou Shintani [新谷創], Lead Security Engineer. Bitcoin World publishes this report and is responsible for its presentation and distribution.

Bitcoin World
bitcoinworld.news