Coded House LLC requested preparation of this auditor-review package for the CodeX (CDX) Ethereum Mainnet contracts. The supplied project evidence has been organized here for independent security-auditor review.

The primary token proxy is 0x27DdDb492c9e593472D28722ED762c04f3d7221f. The contract modules included in scope are CodeXTokenV1.sol, ReserveOracleV1.sol, ReserveManager.sol, FundRegistry.sol, InvestorRegistry.sol, ComplianceManager.sol, AuditManager.sol, SignerRegistry.sol, RedemptionManager.sol, SettlementManager.sol, OracleRegistry.sol, ChainlinkReserveAdapter.sol, ChainlinkRequestManager.sol, CodeXTokenMintLogic.sol, CodeXTokenRedemptionLogic.sol, and CodeXProxyAdmin.sol.

The review scope covers ERC-20 behavior, UUPS/proxy upgradeability, storage-layout integrity, role separation, EIP-712 authorization and replay protection, minting and redemption controls, reserve/oracle publication, Chainlink request handling, compliance registries, Safe multisig governance, and cross-module protocol linking. The independent auditor must confirm the exact source commit/hash before issuing a final signed opinion.

Issues

Critical

None

High

None

Medium

None

Low

[L01] Public documentation and current on-chain reserve state must remain synchronized

The latest supplied on-chain state reports reserveVersion 7, totalSupply 456,500,000 CDX, collateralRatio 200.00% (20,000 bps), availableReserve EUR 456,500,000, lastSnapshotAt 18 August 2026 at 18:26 UTC, and reserveStatus=false. Any public PDF, dashboard, token page, or transparency record that labels older version-4 values as current can create a material consistency issue for reviewers.

Update: The public documentation package has been revised to distinguish historical reserve-version-4 evidence from the later version-7 on-chain state. An independent auditor should reproduce the live reads at its own cut-off block and confirm that the website and final report use the same timestamped values.

Notes

- **UUPS / upgrade authority.** The CodeX deployment uses proxy/UUPS patterns. The supplied evidence reports successful upgrade testing and preserved storage layout. The final auditor should verify implementation slots, initializer protection, _authorizeUpgrade restrictions, ProxyAdmin/Safe authority, and storage compatibility across implementation revisions.

- **Role separation.** Administrative and operational responsibilities are separated across the 3-of-5 Safe, authorized EIP-712 signer, Chainlink node, fund manager, and deployer roles. The final audit should reproduce all AccessControl role memberships and verify that no single operational key can independently bypass issuance or upgrade controls.

- **EIP-712 authorization.** Reserve and mint authorization evidence uses the CodeXReserveOracle EIP-712 domain, Ethereum chain ID 1, the ReserveOracle verifying contract, and an authorized signer. Signatures should bind the exact request fields, chain, contract, amount, fund identifier, expiry, UID/request ID, and reserve version.

- **Replay protection.** UID, nonce, request-ID and processed-request controls should prevent replay of reserve updates and mint approvals. The final auditor should test duplicate submissions, expired approvals, wrong-chain signatures, wrong-contract signatures, altered recipients, and altered amounts.

- **Mint controls.** Minting is expected to require a valid fund, active mint permission, sufficient reserve availability, valid authorization, supply-limit checks, and successful signer recovery before token issuance.

Contract Scope

Component	Ethereum Mainnet address
CodeXTokenV1	0×27DdDb492c9e593472D28722ED762c04f3d7221f
ReserveOracleV1	0×2C2f3583a68b0Ca1eD5D0d3cbDFBabF9D9430Bb2
ReserveManager	0×5e8b1509EB058d0aA107707Ca3540284EAC5A8aD
FundRegistry	0×020A65d5439ac8f1541fcebE16006Ee2ee65e060
InvestorRegistry	0×779E3E56a64FCEA5000F7313Ae462FEdCDdfb2Df
ComplianceManager	0×9cB52fB651A1888b544E1c14C8c185e185453E91
AuditManager	0xB63a6cFB9248587Bb3db5E04D9715463b13CA8Ca
SignerRegistry	0xD7375247217cC82909c1bEF3E848bd07771C9E16
RedemptionManager	0×856e38E8eDa1dD92A36310dE141615352A98622E
SettlementManager	0xA67C92D75eEa91dBb579bdb95b6Bc59Cea92F1F9
OracleRegistry	0xfA40F4b611e5743dD69f81E20F48DD60ef12E417
ChainlinkReserveAdapter	0xd1312BB0677137dc0410E79D003D9c6426D481ad
ChainlinkRequestManager	0×84501e118066B38Df0b90C43C1e67bb897cBbdBE
CodeXTokenMintLogic	0×676B226071E362E3344d1B4A381Fd64D5398dd76
CodeXTokenRedemptionLogic	0xd041b346cbfcb795d3243d557e6096d5Ca1b1A51
CodeXAdmin	0×16035b6eFe7884817D83C4E1e711538736EB7ba2

- **Burn and redemption.** Direct burn and burnFrom are documented as blocked; burn-for-redemption is routed through the controlled RedemptionManager / SettlementManager lifecycle. The independent auditor should test unauthorized direct burn paths, role boundaries, double-redemption and settlement replay.

- **Compliance controls.** InvestorRegistry and ComplianceManager are intended to enforce wallet authorization and transfer/mint/redemption restrictions. Tests should include unauthorized sender/recipient combinations, revoked permissions, paused states and role changes.

- **Signing module.** The supplied operational evidence identifies SoftHSM2 / PKCS#11 as a software signing module. It must not be represented as a certified physical hardware HSM unless separately supported.

Reserve / Oracle Review Notes

• **Current on-chain state.** The latest supplied state is reserveVersion 7, totalSupply 456,500,000 CDX, collateralRatio 200.00% (20,000 bps), availableReserve EUR 456,500,000, lastSnapshotAt 18 August 2026 at 18:26 UTC, and reserveStatus=false. The reported total reserve amount remains EUR 913,000,000.

• **Historical evidence.** Version-4 reserve evidence, Chainlink relay transactions, Safe execution records, hashes and earlier 228,250,000 CDX / 400% values should be retained only as timestamped historical evidence and must not be labelled as the current state.

• **Reserve source wording.** The project evidence describes an authenticated Bank API workflow. The internal service reference 'm1-corebanking' is an application/service name and is not evidence of direct access to a bank's internal core-banking platform.

• **External banking claims.** This smart-contract review does not independently confirm any bank balance, SWIFT message, custodian statement, bank guarantee, or external auditor attestation. Those matters require separate authentic third-party evidence.

• **Chainlink publication.** The adapter/request-manager flow should be tested for caller authorization, request replay, malformed payloads, duplicate request IDs, stale reserve versions, signature mismatch, and failed forwarding into ReserveOracleV1.

• **Reserve freshness.** reserveStatus=false at the supplied cut-off should be interpreted according to the contract's freshness logic. The final auditor should reproduce the exact read at a documented block and determine whether the false state is an expected staleness flag or indicates another condition.

• **Safe governance.** The Safe address is 0xA86FC207De7EDb198a53C7cca179d75Bbeff5C28 with a reported 3-of-5 threshold. Auditor testing should confirm owner set, threshold, upgrade authority, administrative role grants, and representative executed governance transactions.

• **Evidence integrity.** Final publication should identify the audited source commit, compiler/settings, deployment addresses, test suite results, static-analysis output, and report hash. Public PDFs and website values should be reconciled to the same on-chain cut-off.

Update: The CodeX documentation package has been revised to remove prior contradictory/current-state labels and to separate historical reserve snapshots from later on-chain values. Independent auditor verification is still required before this document can become a signed third-party security audit.

Conclusion

No critical, high, or medium issues were found. Some changes were proposed to follow best practices and reduce the potential attack surface. Overall, the code was well written and void of any serious flaws.

Auditors:

Chris Whinfrey

September 16, 2026

Shane Fontaine

September 16, 2026