

CodeX Protocol

Institutional EUR Reserve-Linked Token

OFFICIAL WHITEPAPER

Version 1.3 | September 2026 | Live on Ethereum Mainnet

Published by Coded House LLC

Wyoming, United States | Entity ID 2026-002065283

Corporate history: Coded House Pakistan business presence since July 2024 | Wyoming LLC formed August 2026
codedhouse.com

Publication note: This whitepaper describes the CodeX protocol and its current production architecture. It is a technical and informational document, not an audit opinion, bank statement, prospectus, offering memorandum, deposit certificate, or regulatory approval.

Document Control

Field	Value
Document	CodeX Protocol - Official Whitepaper
Document ID	CDX-WP-1.3
Version	1.3
Publication	September 2026
Publisher	Coded House LLC (Wyoming, United States) - later U.S. entity formed August 2026
Project / Token	CodeX (CDX)
Network	Ethereum Mainnet
Official Website	codedhouse.com
Status	Live on Ethereum Mainnet
Pakistan business presence	Coded House - FBR Registration No. 3740577028434 - earlier/original business presence; acquisition record 1 July 2024
Pakistan registration holder	MUNNAZA USMAN (individual taxpayer / owner)

Source discipline: This official version replaces unsupported statements in the earlier working draft. In particular, it does not identify a named bank or custodian, does not claim direct access to a bank's internal core-banking platform, does not claim an independent audit or regulatory licence, and does not describe SoftHSM2 as a physical hardware HSM.

Contents

- 1. Executive Summary
- 2. Design Objectives
- 3. Protocol Architecture
- 4. Reserve Publication and Proof-of-Reserve
- 5. CDX Token Model
- 6. Minting, Transfers and Redemption Controls
- 7. Governance and Security
- 8. Current Production Status
- 9. Transparency and Public Verification
- 10. Legal Entity and Compliance Approach
- 11. Risk Factors and Limitations
- 12. Roadmap
- 13. Public Technical References
- 14. Disclaimer

1. Executive Summary

CodeX is a permissioned institutional token protocol deployed on Ethereum Mainnet. The protocol is designed for settlement workflows in which token issuance, reserve data, participant eligibility, cryptographic authorization and administrative control can be verified independently at different layers of the system.

CDX is denominated on a EUR 1 nominal-unit basis within the protocol. Minting is conditioned on reserve data received through an authenticated Bank API workflow, recorded through the private ledger and reserve-control stack, signed using EIP-712 typed data, and published to Ethereum through a Chainlink-based relay path. This architecture is intended to reduce the gap between private financial workflows and public-chain verification without exposing confidential credentials or internal banking access.

CodeX does not rely on a single public smart contract for all controls. The production design separates reserve ingestion, private-ledger events, cryptographic signing, oracle publication, token permissions, compliance registries and governance. Administrative actions are controlled through a Safe multisignature wallet with a 3-of-5 threshold.

Current on-chain state: The latest values supplied for this revision report EUR 913,000,000 reserve, 456,500,000 CDX totalSupply, EUR 456,500,000 available reserve, 200% / 20000 bps collateral ratio, reserve version 7, lastSnapshotAt 18 August 2026 18:26 UTC, and reserveStatus=false. The earlier 15 August 2026 version-4 reserve hashes, Chainlink relay and Safe execution remain historical evidence and are not relabelled as version-7 evidence.

What this whitepaper does not claim

- No named bank or custodian is represented as having independently issued or endorsed this whitepaper.
- No SWIFT message, blocked-funds confirmation, bank guarantee or bank statement is represented by this document.
- No independent auditor opinion or assurance conclusion is contained in this whitepaper.
- No blanket statement of regulatory approval, MiCA authorization, EMI licensing or securities-law classification is made.

2. Design Objectives

Institutional tokenization creates a practical problem: public blockchains are transparent and programmable, while financial operations frequently depend on private data, permissioned processes and controlled authorization. CodeX is designed around that tension rather than attempting to remove it.

Objective	Protocol response
Controlled participation	Eligibility and transfer permissions are enforced through registry and compliance contracts rather than assuming unrestricted bearer transfers.
Reserve-aware issuance	Minting depends on reserve state and fund controls instead of a simple administrator mint function.
Privacy with verifiability	Sensitive credentials remain off-chain while hashes, signatures, state transitions and transaction references can be verified publicly.
Role separation	Governance, signing, compliance, reserve publication and fund-management responsibilities are separated across components and addresses.
Operational traceability	Fabric events, request identifiers, Chainlink relay transactions and Ethereum execution receipts create a multi-layer evidence trail.
Upgrade control	Upgradeable modules are governed through controlled administrative permissions rather than unilateral end-user actions.

Design principle: evidence, not disclosure of secrets

The protocol is designed to publish enough information to verify state transitions without publishing API keys, RPC credentials, private keys, PKCS#11 PINs, investor approval codes or other confidential operational material. Public transparency therefore focuses on hashes, signer recovery, contract state, transaction receipts and versioned reserve records.

3. Protocol Architecture

CodeX uses a hybrid architecture. Private and public components have different responsibilities and are deliberately separated.

3.1 Architecture at a glance

Layer	Primary components	Role
Reserve source	Authenticated Bank API workflow	Provides the reserve payload used by the application workflow. Authentication credentials remain confidential.
Private control layer	Hyperledger Fabric (m1-channel, chaincode m1cc v1, sequence 6)	Records permissioned reserve and operational events and provides an internal traceable event layer.
Signature layer	SoftHSM2 / PKCS#11 software signing module	Produces EIP-712 signatures using an authorized signer key without publishing the private key.
Orchestration	Go relayer + Chainlink node	Coordinates reserve refresh requests and relays encoded reserve data toward Ethereum.
Public chain	Ethereum Mainnet smart contracts	Stores reserve state, token supply and permissions in publicly readable contracts.
Governance	Safe multisig	Controls administrative actions using a 3-of-5 owner threshold.

3.2 Core Ethereum contracts

Contract	Address	Function
CodeXToken	0x27Ddb492c9e593472D28722ED762c04f3d7221f	ERC-20 token logic with controlled minting, burning and permission checks.
ReserveOracle	0x2C2f3583a68b0Ca1eD5D0d3cbDFBabF9D9430Bb2	Stores reserve snapshots and exposes reserve state/version information.
ReserveManager	0x5e8b1509EB058d0aA107707Ca3540284EAC5A8aD	Tracks fund reserve, locked reserve and reserve-version state.
FundRegistry	0x020A65d5439ac8f1541fcebE16006Ee2ee65e060	Registers funds and associated configuration.
InvestorRegistry	0x779E3E56a64FCEA50007f313Ae462FEdCDdfb2Df	Stores participant eligibility/registration controls.
ComplianceManager	0x9cB52fb651A1B88b544E1c14CBc1B5e1B5453E91	Applies transfer and transaction policy checks.
SignerRegistry	0xD7375247217cC82909c1bEF3E848bd07771C9E16	Maintains authorized signing identities.
ChainlinkReserveAdapter	0xd1312BB0677137dc0410E79D003D9c6426D481ad	Receives reserve relay data and forwards authorized snapshots.
ChainlinkRequestManager	0x84501e118066B38Df0b90C43C1e67bb897cBbdBE	Tracks reserve-publication requests and responses.

Verification note: Contract addresses are included so reviewers can distinguish the official CodeX deployment from other projects using similar names or symbols. Always verify the contract address before interacting with CDX.

4. Reserve Publication and Proof-of-Reserve

CodeX uses a technical reserve-publication process that links an authenticated Bank API workflow to versioned on-chain reserve state. The process is designed to make the published state cryptographically and transactionally traceable. It should not be confused with an independent bank confirmation or external assurance engagement.

4.1 Reserve publication flow

Step	Process
1	A reserve refresh is initiated and associated with a unique request identifier.
2	The application obtains the current reserve payload through the authenticated Bank API workflow.
3	A related private-ledger event is recorded through Hyperledger Fabric. The production chaincode is m1cc version 1, sequence 6 on channel m1-channel.'
4	The reserve payload is normalized for contract encoding and linked to cryptographic evidence fields.
5	An EIP-712 signature is verified against the authorized signer 0x0CD6265c14049dda2E2a46CC847045c1EB9b9F5F using domain CodeXReserveOracle version 1 and Ethereum chain ID 1.
6	The Chainlink-based publication path relays the reserve payload to the ChainlinkReserveAdapter.
7	An authorized forward action publishes the reserve snapshot to ReserveOracle on Ethereum Mainnet.
8	ReserveOracle and ReserveManager expose the resulting versioned state for public verification.

4.2 Current reserve evidence

Measure	Value
Fund ID	GBP6JX0L73Q4WA6838
Reserve version	7
Reported reserve	EUR 913,000,000
Current utilized / reserved amount (derived)	EUR 456,500,000 - derived as reserve minus available
Current available reserve	EUR 456,500,000
Current on-chain totalSupply	456,500,000 CDX
Current collateral ratio	200% / 20000 bps
Historical version-4 reserve hash (15 Aug evidence)	0x48d8abad0f1326b6c1c737a06043327c98fb8eb67cb718987356c7b2fd5e9665

Meaning of Proof-of-Reserve in CodeX: In this whitepaper, Proof-of-Reserve refers to the protocol's technical evidence chain for reserve data, signatures, versioning and on-chain publication. It is not described as an independent audit opinion

or a bank-issued attestation.

5. CDX Token Model

5.1 Token properties

Attribute	Current specification
Name	CodeX
Symbol	CDX
Network	Ethereum Mainnet
Chain ID	1
Decimals	18
Official token contract	0x27DdDb492c9e593472D28722ED762c04f3d7221f
Nominal denomination	1 CDX represents one EUR-denominated protocol unit
Current on-chain totalSupply	456,500,000 CDX

The nominal EUR denomination describes the unit used by the protocol. It does not, by itself, constitute a bank deposit, bank guarantee, insured account balance, or unconditional redemption promise. Any legal redemption right must arise from separately documented contractual and regulatory arrangements.

5.2 Supply controls

- Minting requires the applicable fund to be active and mint permission to be enabled.
- Reserve state and reserve-version checks form part of the issuance control path.
- The mint authorization is signed and verified against an authorized EIP-712 signer.
- The protocol checks configured supply and transaction limits before mint completion.
- The latest on-chain values supplied for this revision report a CodeXToken totalSupply of 456,500,000 CDX against a reported reserve amount of EUR 913,000,000. The ReserveOracle reserve version is 7, availableReserve is EUR 456,500,000, collateralRatioBps is 20000 (200%), lastSnapshotAt is 18 August 2026 18:26 UTC, and reserveStatus is false.

5.3 Transfer permissions

CDX is designed as a permissioned token. Participant eligibility is handled through registry and compliance components, allowing transfer policy to be enforced at the smart-contract layer. The presence of these controls should not be read as a blanket claim of compliance with every law or regulatory regime; legal eligibility remains jurisdiction- and transaction-specific.

6. Minting, Transfers and Redemption Controls

6.1 Minting sequence

Stage	Control
Eligibility	The destination participant must satisfy the applicable registry and compliance checks.
Fund control	The relevant fund configuration must permit minting.
Reserve control	A valid reserve snapshot/version must be available to the issuance path.
Authorization	A typed EIP-712 mint authorization is signed by the configured signer.
On-chain verification	The token contract recovers and verifies the signer and enforces protocol checks.
Settlement on Ethereum	Upon successful checks, CDX is minted and the resulting transaction/event becomes part of the public chain history.

6.2 Transfers

Transfers are intended for authorized wallets. InvestorRegistry and ComplianceManager provide the on-chain policy layer used to determine whether a transfer is permitted. Off-chain onboarding and identity procedures remain separate from the public chain and may evolve as operational requirements change.

6.3 Redemption

RedemptionManager and SettlementManager contracts are deployed in the production contract suite. This whitepaper does not represent a public redemption service as active unless and until the applicable operational, banking, legal and compliance processes are formally activated and published. The presence of deployed contracts should not be interpreted as a current promise of immediate EUR redemption.

Why this distinction matters: The earlier working draft described bank wire execution and completed redemption as if already operational. Those statements are not carried into this official whitepaper because the available evidence does not support making that public claim.

7. Governance and Security

7.1 Multisignature governance

Administrative control is assigned to Safe address 0xA86FC207De7EDb198a53C7cca179d75Bbeff5C28 using a 3 of 5 threshold. The Safe is used for high-impact administrative actions such as role management, upgrades and fund-registration controls. Separating governance from day-to-day relay and signing functions reduces reliance on a single operational key.

7.2 Cryptographic signing

The current signing environment uses SoftHSM2 through a PKCS#11 interface. SoftHSM2 is a software signing module; this whitepaper therefore does not describe it as certified physical HSM hardware. EIP-712 typed-data signatures provide deterministic message structure and allow the expected signer to be recovered and checked on-chain.

EIP-712 field	Value
Domain name	CodeXReserveOracle
Domain version	1
Chain ID	1
Verifying contract	0x2C2f3583a68b0Ca1eD5D0d3cbDFBabF9D9430Bb2
Authorized signer	0x0CD6265c14049dda2E2a46CC847045c1EB9b9F5F

7.3 Role separation

- Safe owners control administrative governance.
- The EIP-712 signer authorizes reserve and mint messages.
- The Chainlink node and relayer perform publication/orchestration functions.
- Registry and compliance contracts enforce participant and transaction policy.
- Fabric provides a permissioned event and operational record layer.

7.4 Security boundaries

Public verification is built around addresses, hashes, signatures, transaction receipts and contract state. Operational secrets are deliberately excluded. Security therefore depends both on on-chain controls and on disciplined key management, access control, software deployment and incident response outside the blockchain.

8. Current Production Status

The table below distinguishes evidence-backed production status from features that should not be described as complete without separate evidence.

Capability	Status	Evidence / qualification
Ethereum Mainnet contract suite	Live	Official CodeXToken and reserve-control contracts are deployed on Ethereum Mainnet.
Safe governance	Live	3-of-5 multisignature governance configuration supplied.
Fabric reserve event layer	Live	m1cc committed version 1, sequence 6; reserve refresh transaction evidence supplied.
PKCS#11 / EIP-712 signing	Operational	Signer recovery matched the configured signer in the supplied reserve verification evidence.
Chainlink reserve relay	Operational	Production relay transaction 0x2424b8f8e6cd1f5b95733adad6b7d1bea8e7a3f22262964e70f26427c6e8413f was successful in block 25763168.
Safe reserve forwarding	Operational	Execution transaction 0x0e68cbe96c351a9b3d403b240b2bade4a5848471551028ac9dd74d45395e24e8 succeeded in block 25763274.
Reserve-version alignment	Current ReserveOracle version: 7	Latest supplied live-state update confirms ReserveOracle version 7. ReserveManager and CodeXToken reserve-version fields were not separately supplied for this update; no 7/7/7 claim is made.
Redemption contracts	Deployed	Deployment is evidenced; active public redemption service is not asserted.
Independent reserve assurance	Not asserted	No signed external assurance opinion is included in the current public evidence set.
Regulatory licence / authorization	Not asserted	This whitepaper makes no claim of EMI, MiCA or equivalent authorization.

Operational accuracy: Status labels in this section are intentionally conservative. A deployed contract is not automatically treated as an active commercial service, and a technical verification record is not treated as an independent assurance opinion.

9. Transparency and Public Verification

CodeX transparency is based on reproducible public-chain references combined with published technical evidence. A reviewer should be able to start from the official token address, identify the reserve contracts and governance address, and follow the reserve-publication transactions without receiving private credentials.

9.1 Key public references

Reference	Value
Official CDX token	0x27DdDb492c9e593472D28722ED762c04f3d7221f
ReserveOracle	0x2C2f3583a68b0Ca1eD5D0d3cbDFBabF9D9430Bb2
ReserveManager	0x5e8b1509EB058d0aA107707Ca3540284EAC5A8aD
Safe governance	0xA86FC207De7EDb198a53C7cca179d75Bbeff5C28
Chainlink adapter	0xd1312BB0677137dc0410E79D003D9c6426D481ad
Reserve request ID	0x5e74952ef4fdce44dc61d9022df1595aeaa8bd0a170a82109f2250dbc44e3642
Chainlink relay transaction	0x2424b8f8e6cd1f5b95733adad6b7d1bea8e7a3f22262964e70f26427c6e8413f
Safe execution transaction	0x0e68cbe96c351a9b3d403b240b2bade4a5848471551028ac9dd74d45395e24e8
Fabric transaction	7edc785a1461edd8ff54c8e5d513bb49c404b5523e36399c59c28a8de0779b26

9.2 Transparency principles

- Use the official contract address as the primary identity of CDX on Ethereum.
- Publish reserve values with a clear reporting timestamp and version.
- Keep management-reported reserve figures distinct from independent assurance, if independent assurance is obtained later.
- Keep safeTxHash distinct from the mined Ethereum execution transaction hash.
- Do not expose credentials to prove that an API integration exists.
- Do not use cryptographic field names such as auditHash to imply that an external audit has occurred.

Public source-code verification and token-information approval on third-party explorers are separate processes. This whitepaper supports project transparency but does not imply approval, endorsement or regulatory validation by an explorer or infrastructure provider.

10. Legal Entity and Compliance Approach

10.1 Legal entity

Field	Value
Legal entity	Coded House LLC
Entity type	Limited Liability Company
Jurisdiction	Wyoming, United States
State Entity ID	2026-002065283
Principal address	30 N Gould St Ste R, Sheridan, Sheridan County, WY 82801, US
Wyoming Certificate of Good Standing ID	106838024
Certificate date	27 August 2026
Official website	codedhouse.com
Pakistan business presence	Coded House
Pakistan FBR registration no.	3740577028434
Pakistan registration holder	MUNNAZA USMAN - Individual / Owner
Pakistan tax office	RTO Islamabad
Pakistan income-tax / ATL status	Active (ATL checked 11 September 2026)
Pakistan address	Islamabad, Pakistan - full registered address in supporting FBR certificate
Pakistan legal-form note	Supplied FBR records show a business/branch name under an individual taxpayer; separate Pakistani corporate incorporation is not asserted.
Wyoming portal formation date	24 August 2026
Wyoming certificate statement date	25 August 2026
Wyoming Good Standing certificate issued	27 August 2026 at 5:45 AM
Pakistan Coded House business acquisition record	1 July 2024
Pakistan taxpayer registration record	9 July 2024

The corporate history is chronological: Coded House in Pakistan predates the Wyoming LLC. The supplied Federal Board of Revenue records list Coded House as a business/branch under taxpayer MUNNAZA USMAN and show a business acquisition record dated 1 July 2024. The taxpayer registration record is dated 9 July 2024. Coded House LLC is the later U.S. legal entity; the formation-service portal record shows a formation date of 24 August 2026, and the Wyoming Secretary of State Certificate of Good Standing confirms the LLC is in existence and in good standing and was issued on 27 August 2026 at 5:45 AM. CodeX is the project/token name. The source records do not by themselves establish that the Pakistan business is a separate incorporated company or that a parent/subsidiary or legal-succession relationship exists between the two registrations.

10.2 Compliance architecture

CodeX includes technical controls intended to support permissioned institutional workflows, including participant registries, policy checks, separated roles and auditable transaction records. These controls are part of the protocol design; they do not constitute a legal opinion that a transaction or participant satisfies every applicable regulatory requirement.

10.3 External reports

Legal opinions, compliance reports, security assessments and independent assurance reports are separate professional documents. They should only be described as independent, audited, certified or regulator-approved when the relevant qualified third party has actually issued that conclusion.

Whitepaper ownership: This September 2026 whitepaper is published by Coded House LLC, the later U.S. legal entity formed in August 2026. The Coded House business presence in Pakistan predates that LLC and is recorded in FBR records from July 2024 under Registration No. 3740577028434. This whitepaper is not issued by an auditor, bank, custodian, regulator, Chainlink, Safe, Etherscan or any other third party.

11. Risk Factors and Limitations

Risk	Description
Reserve-source risk	The protocol depends on reserve data obtained through an authenticated Bank API workflow. API availability, data quality, permissions or upstream operational changes can affect the workflow.
Key-management risk	Compromise, misuse or loss of signing or governance keys can affect protocol operations. Multisignature and role separation reduce but do not eliminate this risk.
Smart-contract risk	Audited or reviewed code can still contain defects. Upgradeable architecture also creates governance and implementation risk.
Oracle and relay risk	Reserve publication depends on off-chain orchestration and Chainlink-based relay components. Delays or failures can cause on-chain reserve state to become stale.
Liquidity and market risk	A nominal EUR denomination does not guarantee secondary-market liquidity or a market price of exactly EUR 1.
Redemption risk	A deployed redemption contract does not itself create a legal or operational right to receive EUR. Redemption depends on separately activated processes and terms.
Regulatory risk	Digital-asset, payments, securities, AML and stable-value-token rules vary by jurisdiction and may change.
Counterparty and banking risk	Any banking or settlement relationship used operationally can be subject to counterparty, access, policy and service-availability risk.
Technology concentration risk	Ethereum, external RPC providers, Chainlink infrastructure, private-ledger infrastructure and other dependencies may experience outages, congestion or security incidents.
Documentation risk	Public figures can become outdated. Users should verify current contract state and current published reserve evidence rather than relying on a historical whitepaper snapshot.

12. Roadmap

The roadmap focuses on verifiability and operational maturity rather than presenting regulatory or commercial milestones as complete before evidence is available.

Area	Current position	Next focus
Core protocol	Ethereum contract suite deployed	Maintain versioned upgrades, testing and public source verification.
Reserve transparency	Historical version-4 publication evidence retained; latest supplied ReserveOracle state is version 7	Publish a stable transparency page with current timestamps, versions, transaction links and downloadable evidence.
Private ledger	Fabric chaincode active	Strengthen operational monitoring, retention and evidence export.
Signing	PKCS#11 / EIP-712 operational	Formalize key lifecycle, rotation and recovery controls appropriate to production risk.
Governance	Safe 3-of-5 active	Maintain documented owner governance, change management and incident procedures.
Redemption	Contracts deployed; public service not asserted	Activate only when legal, banking, compliance and operational procedures are complete and published.
Independent assurance	Not currently asserted	Engage a qualified independent practitioner if external reserve assurance is required.
Regulatory work	No licence claim in this whitepaper	Continue jurisdiction-specific legal analysis before making regulated-service claims.

13. Public Technical References

The following references identify the production evidence discussed in this whitepaper. Long-form reserve evidence and management reporting should be published separately in the CodeX transparency/documentation area.

Item	Reference
Token contract	0x27DdDb492c9e593472D28722ED762c04f3d7221f
ReserveOracle	0x2C2f3583a68b0Ca1eD5D0d3cbDFBabF9D9430Bb2
ReserveManager	0x5e8b1509EB058d0aA107707Ca3540284EAC5A8aD
Safe governance	0xA86FC207De7EDb198a53C7cca179d75Bbeff5C28
ChainlinkReserveAdapter	0xd1312BB0677137dc0410E79D003D9c6426D481ad
ChainlinkRequestManager	0x84501e118066B38Df0b90C43C1e67bb897cBbdBE
Authorized EIP-712 signer	0x0CD6265c14049dda2E2a46CC847045c1EB9b9F5F
Fabric channel	m1-channel
Fabric chaincode	m1cc v1, sequence 6
Reserve request ID	0x5e74952ef4fdce44dc61d9022df1595aeaa8bd0a170a82109f2250dbc44e3642
Reserve hash	0x48d8abad0f1326b6c1c737a06043327c98fb8eb67cb718987356c7b2fd5e9665
Chainlink relay TX	0x2424b8f8e6cd1f5b95733adad6b7d1bea8e7a3f22262964e70f26427c6e8413f
Safe execution TX	0x0e68cbe96c351a9b3d403b240b2bade4a5848471551028ac9dd74d45395e24e8
Legal entity	Coded House LLC - Wyoming Entity ID 2026-002065283; Pakistan business presence: Coded House - FBR Reg. 3740577028434

Recommended public document set

- Official CodeX Whitepaper (this document).
- CodeX Proof of Reserve & Public Technical Verification Record.
- CodeX Management Financial Figures & Reserves Report, clearly labelled management-prepared and not independent assurance.
- Coded House LLC Wyoming Certificate of Good Standing.
- SHA-256 manifest and, when published, content-addressed IPFS references for exact final files.

14. Disclaimer

This whitepaper is provided for technical and informational purposes. It describes the CodeX protocol based on the production information and evidence available at the time of publication. It is not financial, investment, tax, accounting or legal advice.

Nothing in this document constitutes an offer to sell, a solicitation to purchase, a prospectus, an offering memorandum, a bank deposit, a bank guarantee, a payment-service licence, a securities-law determination, or an independent audit or assurance opinion. No statement in this whitepaper should be interpreted as a promise that CDX will maintain a secondary-market price of EUR 1 or that every holder has an unconditional right of redemption.

Digital-asset systems involve smart-contract, market, liquidity, operational, counterparty, key-management, regulatory and technology risks. Prospective institutional users should perform their own technical, legal, financial and compliance assessment before relying on the protocol.

CodeX may evolve through governed software upgrades, policy changes and operational improvements. The official contract addresses and current transparency records should be checked before any transaction.

Official identity: CodeX (CDX) | Current U.S. publisher: Coded House LLC (Wyoming, formed Aug 2026) | Earlier Pakistan Coded House business presence: FBR Reg. 3740577028434 (records from Jul 2024) | Ethereum Mainnet | Official token contract: 0x27DdDb492c9e593472D28722ED762c04f3d7221f | codedhouse.com