

White Paper

Cuvex Blockchain 20250218

Summary

The purpose of this document is to provide an initial overview of the Cuvex Blockchain and its related technologies, including the CUVX utility token, distributed storage, issuance rules, fee payments, governance, and its interaction with smart contracts for the decentralized management of crypto asset inheritances and digital secrets.

This document should not be considered final, nor is it intended to provide low-level technical details. Instead, its goal is to establish the core objectives of the model and serve as a starting point for building the Cuvex Blockchain.

To ensure clarity and conciseness, we focus primarily on the defining and essential features necessary to achieve the stated objectives.

Introduction

Cuvex is designed as a native, fully independent blockchain that is both deflationary and 100% decentralized. It has been specifically created to provide a technological framework for smart contracts governing crypto asset inheritances and digital secrets, managed by Transcend Node. Understanding Transcend Node in detail is crucial to gaining a clear perspective on the Cuvex Blockchain.

The Cuvex Blockchain will require cryptographic data management and block storage capable of handling substantial data loads. Standard inheritance contracts will typically have a size of less than 0.5MB, but the storage model must be designed to support contracts of up to 2MB.

Nodes will be rewarded for performing required network processes through the issuance and distribution of new CUVX tokens. Additionally, Transcend Nodes must conduct Bitcoin block exploration, necessitating interoperability and communication between the Cuvex Blockchain and other blockchains as part of the verification processes that trigger the creation and insertion of new Transcend Node smart contracts into the Cuvex Blockchain.

In summary, the key objectives are to create a streamlined blockchain with robust processes, capable of managing complex smart contracts, deflationary by design, and equipped to handle cryptographic validation processes. Furthermore, it must support blocks with flexible data size requirements, reaching up to 20MB per block as needed by the network.

1. Cuvex Blockchain Design

Feature	Details
Consensus	Proof of Stake (PoS)
Smart Contract Support	Fully functional Cosmos SDK
Smart Contract Language	WASM, CosmWasm
Block Time	Fast, no more than 10 seconds
Scalability	Thousands of transactions per second
Security	Protection against 51% attacks, slashing mechanisms, and fast finality
Governance	On-chain voting system for protocol upgrades, gas fee agreements, Solidarity Staking, etc.
Interoperability	Ability to interact with other blockchains using IBC

2. Proof of Stake (PoS) Consensus

Instead of miners, the network will be secured by Validator and Encryption Nodes, which must stake CUVX tokens.

- **Participation Mechanism:** Validator-encryption nodes are selected to participate in a lottery-based system based on the amount of staked tokens.
 - **Phase 1:** Each node requires **3,990 CUVX tokens**.
 - **Post-launch (12 months later):** Each node requires **399 CUVX tokens**.
- **Rewards:** Issued in the blockchain's native utility token, **CUVX**.
- **Slashing (Penalties):** Validators may lose staked tokens if they act maliciously or become inactive.
- **Delegation:** Users who do not meet the staking requirements can delegate their stake to validator-encryption nodes.

3. Smart Contract Engine

To support complex smart contracts, the blockchain requires a robust execution environment. Therefore, we will implement:

- **WebAssembly (WASM):**

- High efficiency
- Compatible with **Rust, C++, and Go**

4. Transaction Mechanism, CUVX Token Issuance, Fees, and Penalties

Mempool for Signed Transactions and Transcend Node Contract Instantiation

Every transaction between wallets is signed and sent to the mempool, just as each Transcend Node contract is also signed and submitted to the Cuvex blockchain mempool. Both will be available for selection by the winning node in the allocation lottery among all operational nodes based on their staking, allowing them to include the transactions in their processed block.

The allocation lottery, which governs the selection of the **Validator Node** for a block and the **Primary Node** for a Transcend Node contract, is designed to ensure the participation of all nodes, regardless of their staking amount beyond the minimum required. In practice, each winner of the auditable lottery is added to a **rewarded node list** and excluded from the **pending node pool** until all pending nodes have been selected at least once. This process works like an **hourglass rotation** once a node moves to the rewarded side, the lottery continues among the remaining pending nodes. The hourglass is reset only after all nodes have been selected.

This lottery system ensures a fully auditable and transparent process that guarantees the participation of all nodes without exception.

Each request to instantiate a Transcend Node contract is submitted to a **dedicated inheritance contract mempool**, separate from the standard transaction mempool. This separation is necessary because inheritance contracts require an independent lottery mechanism unrelated to Cuvex blockchain block validation and Bitcoin transaction validation timelines.

When a **Primary Node** is selected via the contract lottery and completes verification of a **Transcend Node smart contract**, it signs the contract with its private key and submits the signed contract to the **Cuvex transaction mempool**. The **winning Validator Node** in the standard block validation lottery will then include this contract in the Cuvex blockchain.

The insertion of **Transcend Node smart contracts** into the Cuvex blockchain **does not** result in any CUVX token rewards; it is considered an internal transaction without a Gas Fee.

Two Independent Lotteries and Mempools

1. Cuvex Blockchain Block Validation Lottery

- Winning nodes receive newly minted CUVX tokens via **Coinbase transactions**.
- Additional **CUVX tokens** are rewarded as Gas Fees paid by users.

2. Transcend Node Smart Contract Verification Lottery

- Winning nodes are rewarded **directly in Bitcoin (BTC)** for verifying inheritance contracts.

CUVX Token Issuance

The **CUVX token** has a total supply of **21 million tokens**.

- **Block validation rewards** are the **only** mechanism for issuing new CUVX tokens.
- Rewards **halve every 12,614,400 blocks** (~every 4 years), triggering the **CUVX Halving** event.

Initially, validator nodes will earn approximately **0.6742 CUVX** per validated block.

In the **final issuance phase**, nodes will receive **0.00000000251 CUVX** per validation this will occur approximately **112 years** after the blockchain launch.

At that point, node rewards will be derived from:

- **Gas Fees** from user transactions.
- **Bitcoin (BTC) fees** from participation in **decentralized inheritance contracts (Transcend Node contracts)**.

Valid Block Decision

Cuvex uses the **Tendermint Byzantine Fault Tolerance (Tendermint BFT) protocol**, a **Proof of Stake (PoS)-based consensus mechanism** that prevents chain splits by enforcing **deterministic voting rounds**.

All nodes vote before a block is inserted, ensuring **real-time fork prevention**.

Transaction Fees for Block Inclusion

- The sender of a transaction must pay a **Gas Fee** in CUVX, determined by:
 - **Transaction size (bytes)**
 - **Computational requirements**
 - **Network congestion models**
- The winning **Validator Node** in the block validation lottery receives:
 1. **Newly minted CUVX tokens** via **Coinbase transaction**.
 2. **Gas Fees** paid by users for transaction inclusion.

3% of the Gas Fee from each transaction **is allocated to Cuvex's solidarity staking pool**.

Fees for Transcend Node Processes

Cuvex manages **Transcend Node smart contracts**, which require a **Bitcoin fee** for instantiation.

- **Transcend Node Contract Instantiation Fee:**
 - **\$4.15 USD in BTC** per moth, for contract (up to **0.5MB / 525,000 bytes**)
 - Minimum **4-month latency period** required.
- **Shamir Fragment Decryption & Reconstruction Fee (for inheritance retrieval):**
 - **\$99 USD in BTC** for the first 12 months after the latency period expires.
 - If retrieval occurs **after** 12 months, the fee **increases by \$99 USD in BTC per year**.
 - Fees increase by **2% annually**, automatically enforced by **Transcend Node smart contracts**.

Transcend Node Encryption Challenges

Nodes encrypting **inheritance smart contracts** must pass **encryption challenges** to maintain **Cuvex's operational integrity, resilience, and contract longevity**.

- **Challenges occur every 12 hours** for all nodes participating in inheritance contracts.
- The goal is to **prove node availability** and ensure nodes can **decrypt Shamir fragments** if required.
- A **contract health score** will be visible to the contract issuer via blockchain explorers.

Penalties (Slashing Mechanisms)

The **Encryption Challenge** enforces **slashing penalties** on non-compliant nodes:

- If a node **fails** to meet its challenge obligations, a **portion of its staking balance** is redistributed to **compliant nodes**.
- If a node loses **more than 30%** of its staking balance due to penalties, it **loses eligibility** for inheritance contract lotteries until the balance is restored.
- If a node's staking balance falls **below 50%**, it will face **complete forfeiture** of its stake and be **permanently removed from the network**.

5. Decentralized Governance

The blockchain must evolve without governance-related forks. To achieve this, we will implement **on-chain governance**:

- **Community Voting** → Users who hold sufficient stake to operate a **Transcend Node** will be eligible to vote on protocol upgrades, network improvements, Gas Fees for transactions, and the allocation and use of the **Solidarity Staking Pool**.
- **Restrictions** → The total supply of **CUVX tokens** and the predefined rewards for contract instantiation, renewal, decryption, and recovery of **Transcend Node smart contracts cannot** be altered under any circumstances.

6. Base Code Implementation

Component	Technology
Core Programming Languages	Rust, Go, C++
Blockchain Framework	Cosmos SDK
Database Engine	RocksDB, LevelDB
Smart Contract Languages	Rust (WASM), CosmWasm

7. Genesis Block Creation, Initial Issuance, Maximum Supply, Token Distribution, and Node Deployment

The **Cuvex blockchain** is designed to be **deflationary**, ensuring long-term value appreciation. To achieve this, Cuvex will issue a **fixed total supply of 21 million CUVX tokens**.

These CUVX tokens will be minted in **only two issuance events**:

- **19% (3,990,000 CUVX)** will be issued in the **Genesis Block**.
- The remaining **81% (17,010,000 CUVX)** will be gradually distributed through **block validation rewards**. The winning node in the block validation lottery will include a **Coinbase transaction** in the block it validates, minting a pre-determined token amount based on the block height, as defined by the Cuvex blockchain protocol.

Initial Node List and Staking Requirements

The **initial validator nodes** will consist of early project contributors who receive a portion of the **19% of Genesis-issued tokens** and stake the required amount to deploy a **Transcend Node**.

The total number of operational nodes will be **limited** by the circulating supply of CUVX tokens. However, the network will naturally expand over time as **new tokens are issued through block validation rewards**.

The goal is to establish a **decentralized, redundant, and resilient network** while ensuring that each node remains **economically viable**.

To achieve this, **Cuvex adopts a Bitcoin-like halving model**, where:

- **Every 12,614,400 blocks (~4 years), block validation rewards are halved.**
- This progressive reduction ensures **controlled issuance** and long-term network sustainability.

As outlined in **Section 2**, the **staking requirement for Transcend Nodes** will follow a **two-phase structure**:

1. **Phase 1** (Initial Smart Contract Deployment)
 - **3,990 CUVX tokens** are required to activate a Transcend Node.
 - This phase is **exclusively covered by the 19% of Genesis-issued tokens**.
 - **A maximum of 1,000 nodes** will be operational during this phase.
2. **Phase 2** (12 Months After Official Transcend Node Activation)
 - **399 CUVX tokens** per node will be required.

Initial Parameters

Airdrop Rewards

- **47.36% (1,889,664 CUVX)** of Genesis-issued tokens will be distributed as **rewards for project contributors**.
- A **task-based rewards system** will be established with predefined deadlines, requirements, and rewards. Anyone interested in contributing whether in **technical development, marketing, legal support, or other areas** can complete assigned tasks and receive the corresponding token rewards.
- All reward distributions will be based on the **verification of completed milestones** within a defined timeframe.

Seed Allocation and Private Sales

- **52.64% (2,100,336 CUVX)** of Genesis-issued tokens will be allocated to **Semilla3 LLC**, Cuvex's parent company, to **finance the project and act as the primary promoter**.
- This allocation will support **private and public sales** to third-party investors and will also be used to compensate:

- **The core development team**
- **Advisors**
- **Strategic collaborators**

Detailed token distribution and economic models will be outlined in the project's Tokenomics documentation.

Block Validation Rewards

As previously mentioned, **block validation rewards** will be funded through:

1. **Gas Fees** paid by transaction senders, calculated based on:
 - **Transaction size (bytes)**
 - **Computational complexity**
 - **Network congestion levels**
 - **These parameters will be determined by the consensus of the Transcend Node network.**
2. **Coinbase Transactions** embedded in each validated block by the winning Validator Node, according to issuance rules defined by the **Cuvex blockchain protocol**.

Token Issuance Rules

The issuance of **CUVX tokens** will follow the rules outlined below:

- After the **Genesis Block**, during **Phase 1** of the **Transcend Node deployment**, a **maximum of 1,000 active nodes** will be allowed, forming the initial foundation for token issuance.
- During **Phase 2**, based on the block creation rate, **2,126,250 new CUVX tokens** will be issued annually, enabling the creation of up to **5,329 new Transcend Nodes per year** until the first **Halving event**.
- Over time, the **maximum number of Transcend Nodes** will reach **42,631 active nodes** once the total supply of **CUVX tokens** has been fully issued.

As stated in **Section 4**, initially, nodes will receive **0.6742 CUVX per block validation**. In the final issuance phase of the **deflationary CUVX token**, nodes will receive **0.00000000251 CUVX per block validation**.

The **total supply of CUVX tokens** is **21 million**, with:

- **19% issued in the Genesis Block**
- **81% issued progressively through block creation and validation**

For reference, an estimated issuance schedule for **the next 115 years** can be found at the following link: [Insert Link].

Block Time

The **block time** will be set based on the technical requirements for transaction validation and allocation calculations. However, it **will not exceed 10 seconds** under any circumstances.

For **Transcend Node smart contract instantiation**, a **minimum of four Bitcoin blockchain confirmations** will be required before the contract is fully recorded on the **Cuvex blockchain**.

Slashing Policy

The **Cuvex blockchain** prioritizes **operational reliability, persistence, resilience, security, and censorship resistance**. To uphold these principles, strict **penalties** will be enforced for nodes that:

- Operate intermittently
- Fail encryption challenges
- Engage in fraudulent activities

While additional penalties will likely be introduced during development, the following obligations are **mandatory** for nodes. Any failure to comply will result in penalties:

Primary Node Responsibilities in Transcend Node Smart Contracts

The **winning node** of the lottery for **contract instantiation, renewal, or recovery** must:

1. **Verify its lottery selection** by attaching the **lottery ID** to the contract. This ID is provided by the **smart contract managing the Transcend Node mempool assignment**.
2. **Sign the Bitcoin reward address** using its **RSA private key**, allowing other nodes to verify it.
3. **Ensure data integrity** by confirming that all **user-submitted contract data** is correctly formatted for:
4.
 - Decryption

- Verification
 - Future reconstruction of the **Shamir secret-sharing scheme** for the designated heir
 - This verification must also be performed by **all encryption nodes** linked to the Transcend Node smart contract.
5. **Wait for four Bitcoin confirmations** before signing and inserting the contract into the Cuvex blockchain.
 - If a node attempts to process the contract **before receiving four confirmations, validator/encryption nodes will reject it**, triggering a **penalty** for the Primary Node.
 6. **Sign the verified contract** with its **RSA private key** before submitting it to the Cuvex transaction mempool.

Encryption, Verification, and Validation Nodes Linked to Transcend Node Contracts

To approve a contract's submission to the Cuvex transaction mempool, a vote must be conducted by 369 linked nodes. These nodes are responsible for:

- **Validating** each step taken by the Primary Node before the contract is **signed** and **proposed for inclusion in the mempool**.
- **Performing additional verifications** when the **Bitcoin reward payment block height** reaches maturity.
- Ensuring that the **Primary Node** completes the process **on time and according to protocol**.
- If the **Primary Node fails** to fulfill its duties, verification nodes will **take over the contract verification** according to the order of assignment.

If the **smart contract detects that the Primary Node has only partially or completely failed** in its duties, and another verification node **completes the process instead**, the **Primary Node will be penalized** by losing **1% of its staked CUVX tokens**.

Winning Node in the Cuvex Blockchain Block Validation Lottery

The **winning Validator Node** in the **block validation lottery** must:

1. **Construct the block** for validation, including its **Coinbase transaction** according to **network rules**.
2. **Validate** all transactions within the **mempool** before including them in the block.
3. **Validate** all smart contracts in the **Cuvex blockchain mempool** that have passed prior verification steps.

The **entire work of the winning Validator Node** will be:

- **Audited by the Cuvex blockchain compliance system**
- **Re-validated by all nodes before final acceptance into their local chains**

Node Responsibilities for Receiving Transactions or Transcend Node Contracts

Any **node receiving a transaction or Transcend Node contract** is required to **validate its parameters** before including it in its own **mempool**, as doing so would propagate the transaction across the network.

Validation procedures include:

- **Data structure verification**
- **Cryptographic signature verification**
- **For Transcend Node contracts:** Verification of the **Bitcoin transaction ID (BTC TxID)**

This ensures that **spam transactions** or **denial-of-service (DoS) attacks** are not introduced into the **Cuvex blockchain mempools**.

Slashing Procedures Enforced by the Transcend Node Smart Contract, Cuvex Compliance Systems, or Validator Nodes

The **Transcend Node smart contract** is responsible for ensuring that **each participant fulfills their assigned tasks**.

Failure to execute any **required task** will result in **immediate slashing** of **CUVX tokens**, according to the network's **governance policies**.

- **Minor Infractions:**
 - If a node incurs **small penalties** (losing **1% of its staked tokens**) and accumulates a **30% loss** of its total **staked CUVX**, it will be **excluded from Transcend Node inheritance contract lotteries**.
 - However, it will still be allowed to **participate in block validation lotteries** until it restores its staking balance.
- **Major Infractions (50% Loss Penalty):**
 - If a node accumulates **50% staking losses**, it will face **complete slashing** of its **staked CUVX** and **permanent expulsion from the Cuvex blockchain**.

- **Severe Fraudulent Activities:**
 - Nodes engaging in **critical violations** that threaten network security such as:
 - **Double-signing**
 - **Altering the Coinbase transaction**
 - **Any other severe action that compromises blockchain integrity**
 - Will **immediately lose 50% of their staked CUVX** and be **permanently removed from the network**.

Genesis Block Unique Message

"The unrestricted respect for the life project of others, based on the principle of non-aggression, in defense of the right to life, liberty, and private property."

8. Security and Attack Resistance

As an **initial introduction**, to **maximize security** and mitigate **51% attacks, Sybil attacks, and other threats**, we will implement the following measures, among many others that will emerge during the technical development phase:

- **Slashing: Penalties for Dishonest Validators**
 - As detailed in the **previous section**, we will enforce **strict slashing penalties** to **deter fraudulent behavior, validator inactivity, or failure to fulfill node responsibilities**.
 - This system will be deployed so that:
 - **Smart contracts autonomously report violations.**
 - **Other nodes can also report fraud and receive rewards.**
 - **A central on-chain auditing mechanism** will oversee all security processes.
- **Fast Finality**
 - We will implement **Tendermint** to ensure **transaction finality within seconds**.

9. Wallets and User Tools

For blockchain adoption to **succeed**, it must offer **exceptional user experience tools**. Fortunately, **Cuvex has already undergone years of development** in its initial phase:

- **Official Wallet**

- The **Cuvex App** is already a **PSBT Watch-Only Wallet with Double Airgap**.
- Building upon this, we will develop the **official Cuvex Wallet** and integrate it with **Cuvex hardware devices** to facilitate the **generation of custom seed phrases for CUVX tokens**.
- This will be essential for both **node operators and end users**.
- **Block Explorer**
 - One viable option is to **adapt Etherscan** for our blockchain.
 - However, this is **not a final decision**, as other promising alternatives are being considered.
- **APIs & SDKs**
 - **Developer integration is a top priority**.
 - We will provide a **comprehensive and well-documented development environment**, enabling seamless integration and allowing anyone to build solutions based on **Cuvex or Transcend Node**.

10. Solidarity Staking

Beyond **efficiently managing decentralized inheritances of crypto assets or digital secrets**, the **Cuvex Blockchain's founding team** strongly believes in leveraging **technology to help alleviate global child suffering**.

- The **Cuvex Blockchain's active node network** will accumulate a **Solidarity Staking Fund**, funded by **3% of all Gas Fees from CUVX transactions**.
- Every month, the **blockchain's governance engine** will **review and propose humanitarian projects** that have undergone **proper verification**.
- Approved projects will receive **funding from the accumulated Solidarity Staking balance**.
- **Eligible projects must focus exclusively on direct aid initiatives aimed at combating:**
 - **Hunger**
 - **Disease**
 - **Child labor**

11. Testnet and Mainnet

Before launching the **Mainnet**, we will first deploy a **Testnet** to identify and resolve potential issues.

- **Faucets** → Free **Testnet tokens** will be distributed for testing purposes.
- **Bug Bounty Program** → Ethical hackers will be invited to discover vulnerabilities and will receive **CUVX token airdrop rewards**.
- **Stress Testing** → We will simulate **high network traffic** to evaluate system performance and scalability.

12. CUVX Tokenomics

- **Total CUVX Supply: 21,000,000 CUVX**
- **Genesis Block Issuance: 19% (3,990,000 CUVX)**
- **Post-Genesis Issuance:**
 - Distributed through **Coinbase transactions** in each validated block.
 - Initial reward: **0.6742 CUVX per block**, reduced by **50% every 12,614,400 blocks** (~every 4 years).

Genesis Block Allocation

- **47.36% (1,889,664 CUVX):** Reserved for **project contributors** as reward incentives.
 - A **task-based reward system** will be implemented, where contributors can complete predefined tasks and receive **CUVX tokens** upon successful verification of their work.
 - Contributions may include **technical development, marketing, legal advisory, and other areas**.
- **52.64% (2,100,336 CUVX):** Allocated to **Semilla3 LLC**, the parent company of **Cuvex**, to finance the project and serve as its main promoter.
 - This allocation will be used for **private and public sales** to third-party investors and to compensate:
 - **The internal development team**
 - **Advisors**
 - **Key collaborators**

CUVX Token Allocation

Category	Allocation
Team	24%
Advisors	1%
Community Rewards	10%
Liquidity Provision	5%
Treasury	10%
Initial Transcend Nodes	20%
Private and Public Sales	30%

Vesting Schedule

- **Year 1 & 2: 19% of the total supply** is released.
- **Year 3 to ~Year 111:** The remaining **81%** will be gradually issued through block validation.