CyberLotto

The Transparent, On-Chain Lottery

Whitepaper · Version 1.9 · April 2026

Built on Base · Powered by Chainlink

Table of Contents

---

1. Legal Disclaimer

This whitepaper is published for informational purposes only. It does not constitute financial, investment, or legal advice, and nothing contained herein should be interpreted as a solicitation or offer to buy or sell any security, token, or financial instrument.

Participation in the CyberLotto protocol involves financial risk. Ticket purchases do not guarantee any return. Prize pools depend on participation volume and may be lower than expected in early rounds. Smart contracts, while audited, may contain unforeseen bugs. Cross-chain operations rely on third-party infrastructure (Chainlink CCIP) and carry the associated risks of bridging protocols.

Users are solely responsible for ensuring that their participation complies with the laws and regulations of their own jurisdiction. CyberLotto is not available in jurisdictions where on-chain lotteries or gambling are prohibited. Regulatory frameworks for blockchain-based gaming vary widely and are subject to change.

The CyberLotto team makes no warranties, express or implied, regarding the accuracy or completeness of this document. The protocol design, tokenomics, and governance parameters described herein are subject to change prior to and after launch.

---

2. Abstract

Lotteries are one of the world's oldest forms of entertainment — but traditional ones have a fundamental problem: you have to trust whoever is running them. CyberLotto is built on a different premise: **the rules are enforced by code, the draws are proven fair by mathematics, and no one — not even the team — can manipulate the outcome.**

CyberLotto is a fully on-chain lottery deployed on the **Base blockchain**. Every lottery ticket is issued as an NFT — a digital token you truly own — all prize calculations happen transparently on the blockchain, and winning numbers are generated using cryptographic randomness that nobody can predict or influence.

Players pick 6 numbers from 1–49, pay 5.20 USDC per selection, and compete for prizes across 6 tiers — from a jackpot worth 67.5% of the prize pool down to free ticket credits for matching just 2 numbers or 1 number plus a bonus. Rounds run twice per week, open automatically, and settle without any manual intervention from the team.

> **CyberLotto is not just a lottery — it is a protocol. All prize funds are locked in a smart contract that only winning ticket holders can access. The team cannot touch them.**

Players on other EVM chains can purchase tickets without leaving their own network. A hub-and-spoke architecture powered by **Chainlink CCIP** routes cross-chain purchases to the lottery's home chain, where tickets are minted directly to the buyer's wallet. If a purchase fails, the USDC is automatically refunded. All other operations — including prize redemption, free ticket claims, and ticket burns — are performed on Base.

---

3. Introduction

Traditional lotteries have three problems that players have simply learned to accept:

- **Opacity.** You have no way to verify that a draw was genuinely random. You take the operator's word for it.
- **Centralization.** A single organization controls everything — the draw, the results, and the money. They could manipulate any of these.
- **Custody risk.** Prize funds sit in accounts controlled by the operator. If the operator disappears or is hacked, your winnings can vanish with them.

CyberLotto resolves all three:

- **Transparent by design.** Every draw, result, and prize calculation is executed on-chain and publicly verifiable. Anyone can audit the full history of the protocol, at any time, without asking permission.
- **Provably fair.** Winning numbers are generated by Chainlink VRF, a service that produces random values alongside a cryptographic proof. The proof is checked on-chain automatically before results are recorded. Nobody — including the CyberLotto team — can predict or alter the outcome.
- **Non-custodial prizes.** Prize funds are held in a smart contract that the team cannot access. Winners redeem directly. There is no intermediary.
- **Decentralized winner counting.** Tallying millions of tickets on-chain in a single transaction is not feasible. Instead, Chainlink's decentralized node network counts winners off-chain, reaches consensus, and submits the result on-chain — preserving trustlessness without the gas bottleneck.
- **Multi-chain access.** Players on other EVM chains can purchase tickets through a local contract on their own network. Chainlink CCIP handles the cross-chain messaging and token transfer. The ticket is minted directly to the buyer's address on Base — no manual bridging required.

---

4. How to Play

Getting started with CyberLotto takes a few minutes. Here is what the experience looks like from start to finish.

Step 1 — Get USDC

CyberLotto accepts USDC as payment. You can participate in two ways:

- **On Base (direct):** Get USDC on Base, along with a small amount of ETH for gas fees, and purchase tickets directly from the main lottery contract.
- **From another chain:** If you hold USDC on a supported spoke chain (such as Ethereum or Arbitrum), you can purchase tickets through the CyberLottoSatellite contract on that chain. You will also need a small amount of the spoke chain's native token (e.g. ETH) to cover the Chainlink CCIP messaging fee, included directly in your purchase transaction.

Step 2 — Pick your numbers

Choose 6 numbers between 1 and 49 for each selection you want to make. You can include multiple selections on a single ticket — each one is priced and scored independently.

Step 3 — Buy your ticket

Each draw selection costs **5.20 USDC** (5.00 USDC goes into the prize pool; 0.20 USDC covers protocol fees). Your ticket is minted as an NFT and sent to your wallet. You can verify it on-chain at any time.

Buying from another chain: If you are on a supported spoke chain, call `purchaseTicket` on the CyberLottoSatellite contract instead. The Satellite validates your numbers locally, pulls your USDC, and sends everything to the hub chain via Chainlink CCIP. Your ticket NFT is minted directly to your wallet address on Base.

Step 4 — Wait for the draw

Rounds close automatically at **02:00 UTC on Thursdays and Mondays**. After closing, winning numbers are drawn using Chainlink VRF within a few minutes. Winner counts are tallied by the Chainlink node network and prizes are locked on-chain shortly after. The draw schedule is controlled by a swappable scheduler contract — CLT holders can propose and vote to change it through DAO governance.

Step 5 — Check and claim your prize

Once a round is settled, you redeem your ticket directly from the smart contract. Prize USDC is sent to your wallet instantly. All redemption, free ticket claims, and ticket burns are performed on Base — if you purchased cross-chain, switch to Base to interact with your ticket NFT.

Prize Tiers at a Glance

Tier	Condition	Prize	Share of Total Pool
1	Match all 6 — Jackpot	Split among winners	67.5%
2	Match any 5 of 6	Split among winners	7.2%
3	Match any 4 of 6	Split among winners	7.2%
4	Match any 3 of 6	Split among winners	8.1%
5	Match any 2 of 6	1,000 free ticket credits	—
6	Match 1 of 6 + bonus	1,000 free ticket credits	—
Reserve	Always retained	Carries to next round	10%

Tiers 5 and 6 award **1,000 free ticket credits** rather than USDC. Players accumulate credits and can redeem them at a rate of **1,000 credits per free ticket** (one draw selection). Free ticket credits do not expire and are tracked per wallet address on-chain. Unclaimed tier prize pools (tiers 1–4) carry forward and grow the next round's jackpot.

Odds of Winning

CyberLotto uses a 6/49 draw format. The following table shows the exact probability of each tier per single draw selection:

Tier	Condition	Odds (1 in …)	Probability
1	Match all 6	13,983,816	0.000007%
2	Match any 5 of 6	54,201	0.0018%
3	Match any 4 of 6	1,032	0.097%
4	Match any 3 of 6	57	1.77%
5	Match any 2 of 6	7.6	13.24%
6	Match 1 of 6 + bonus	12.2	8.17%

The overall chance of winning any prize (tier 1–6) on a single draw selection is approximately **1 in 4.3** (23.2%). These odds are inherent to the 6/49 combinatorial format and are identical to any lottery using the same number pool and draw size. The protocol cannot alter them.

---

5. System Architecture

CyberLotto is built from several smart contracts that work together, supported by four external Chainlink services.

Component	What it does
CyberLottoTickets	The main contract. Holds the prize pool, issues ticket NFTs, runs the round lifecycle, and coordinates with Chainlink VRF, Automation, and CRE.

Component	What it does
CyberLottoLibrary	A pure math library with no stored data. Contains all lottery calculations — validating picks, scoring draws, splitting prizes. Can be audited independently.
CyberLottoScheduler	Determines when each round ends (default: Thu & Mon 02:00 UTC). Implements a standard interface that `CyberLottoTickets` calls to check whether a round should close. CLT holders can propose a new scheduler contract — with a different frequency or timing — and vote to swap it in through DAO governance, without touching the main contract.
CyberLottoHub	Lives on the same chain as CyberLottoTickets. Receives cross-chain purchase requests via Chainlink CCIP and calls the main contract to mint tickets directly to the buyer. Sends USDC refunds if a purchase fails.
CyberLottoSatellite	Deployed on each supported spoke chain. Validates draw selections locally, pulls USDC from the player, and sends a purchase message to the Hub via Chainlink CCIP.
Chainlink VRF v2.5	Generates provably fair winning numbers. Delivers a cryptographic proof alongside each result that is verified on-chain before numbers are accepted.
Chainlink Automation	Monitors round timing. Automatically closes rounds at the scheduled time and opens new ones after prizes settle — no manual action needed.
Chainlink CRE	Counts winners off-chain across a decentralized node network, then submits the result on-chain after reaching consensus. Eliminates the gas bottleneck of counting millions of tickets in a single transaction.
Chainlink CCIP	Transports messages and USDC between spoke chains and the hub chain. Provides source validation, token transfer, and delivery guarantees for cross-chain ticket purchases.

---

6. Game Mechanics

Draw Format

Each draw is a selection of exactly 6 numbers from a pool of 49 (numbered 1 through 49). The contract enforces this at purchase time — any selection with the wrong count or an out-of-range number is rejected immediately.

Ticket Pricing

Each draw selection costs **5.20 USDC**. Of that:

- **5.00 USDC** goes directly into the prize pool.
- **0.20 USDC** (4%) is held as an operational fee for the protocol treasury.

A single ticket can bundle multiple draw selections. A ticket with 3 draws costs 15.60 USDC, with all 15.00 USDC going into the prize pool.

The Draw Result

When a round closes, two independent random values are requested from Chainlink VRF. They are used to produce:

- **Six main numbers** selected from 1–49 using a statistically fair shuffle. Every possible combination has an equal probability of being chosen.
- **One bonus number** selected from the remaining 43, guaranteed never to duplicate any of the six main numbers.

Both values arrive with a cryptographic proof that is verified on-chain. The team cannot know, change, or influence the result.

Front-Running Protection

The VRF request and the VRF result delivery occur in **separate blocks**. When a round closes, the contract submits a randomness request in one transaction; Chainlink VRF fulfils it in a later transaction. Because the winning numbers do not exist until the fulfilment block — after ticket sales have already stopped — no participant can observe the result and purchase tickets based on it.

Scoring

Once the result is published, each draw on every ticket is automatically scored. The contract counts how many of the player's 6 numbers match the 6 main result numbers, and checks separately whether any number matches the bonus. The combination determines the prize tier.

Free Ticket Credits

Tiers 5 (match any 2 of 6) and 6 (match 1 of 6 + bonus) award **1,000 free ticket credits** per qualifying draw. Credits are tracked per wallet address in the contract's on-chain state. Players can redeem credits at a rate of **1,000 credits per free ticket** (one draw selection). Free ticket credits do not expire and cannot be transferred between wallets.

To claim free tickets, a player calls `claimFreeTickets` on the `CyberLottoTickets` contract on Base, specifying draw selections. The contract deducts credits and mints a ticket NFT with no USDC cost. Free ticket draws contribute to the burn-to-earn programme identically to purchased draws.

---

7. Prize Structure

How the Pool Is Split

Each round, **10% of the total prize pool** is set aside as a jackpot seed for the next round — so the jackpot always starts with a meaningful base and grows over time if unclaimed. The remaining **90%** (the "distributable pool") is allocated to winning tiers:

Tier	Condition	% of distributable pool	% of total pool
1	Match all 6 — Jackpot	75%	67.5%
2	Match any 5 of 6	8%	7.2%
3	Match any 4 of 6	8%	7.2%
4	Match any 3 of 6	9%	8.1%
5	Match any 2 of 6	Free ticket credits	—
6	Match 1 of 6 + bonus	Free ticket credits	—
Reserve	Always retained	—	10%

If no tickets win a particular tier in a given round, those funds stay in the pool and increase the following round's jackpot. A quiet round is always good news for the next one.

Claiming Your Prize

Once a round is fully settled, any winning ticket holder calls `redeemTicket` on the smart contract. The contract verifies the ticket, calculates the prize, and sends USDC directly to the NFT owner's wallet. No intermediary is involved. Tickets can only be redeemed once.

---

8. Token Economics

Ticket Pricing Summary

Component	**Amount per draw**
Prize pool contribution	5.00 USDC
Operational fee	0.20 USDC
Total player pays	**5.20 USDC**

Jackpot Carry-Forward

The 10% jackpot seed never leaves the pool in the round it is earned. It forms the base of the next round's jackpot. Unclaimed tier prizes (from tiers with zero winners) also carry forward. Every round starts with an existing prize pool, and the jackpot grows the longer it goes unclaimed.

Governance Token — CLT

CyberLotto Token (CLT) is the protocol's governance and revenue-sharing token, with a hard cap of **1,000,000,000 CLT**. CLT holders can propose and vote on protocol changes, and earn a share of protocol fee revenue by staking.

Tranche	**Amount**	**Notes**
NFT burn rewards	600M CLT (60%)	Minted on demand when tickets are burned
Team	250M CLT (25%)	Pre-minted, subject to vesting
DAO treasury	150M CLT (15%)	Pre-minted, managed by governance

Burn-to-Earn

Once a round is finished and any USDC prizes are claimed, ticket holders can permanently lock their ticket NFT into the **TicketBurnVault** to receive CLT tokens. Rewards are distributed across

10 eras of 5 million draws each, with the rate stepping down every era to reward early participants most:

Era	Total draws burned	CLT per draw	Era total	Cumulative
0	0 – 5M	30 CLT	150M CLT	150M CLT
1	5M – 10M	20 CLT	100M CLT	250M CLT
2	10M – 15M	15 CLT	75M CLT	325M CLT
3	15M – 20M	12 CLT	60M CLT	385M CLT
4	20M – 25M	10 CLT	50M CLT	435M CLT
5	25M – 30M	9 CLT	45M CLT	480M CLT
6	30M – 35M	8 CLT	40M CLT	520M CLT
7	35M – 40M	7 CLT	35M CLT	555M CLT
8	40M – 45M	5 CLT	25M CLT	580M CLT
9	45M – 50M	4 CLT	20M CLT	600M CLT

The burn pool distributes exactly **600M CLT** across 50 million total draws. All rates are whole numbers, making the schedule straightforward to implement and easy for participants to verify. Once era 9 is complete, burning a ticket yields 0 CLT.

---

9. Provably Fair Randomness

The fairness of any lottery lives or dies by the quality of its random draw. CyberLotto uses **Chainlink VRF v2.5** (Verifiable Random Function) — a service designed specifically to provide random values that are both unpredictable and independently verifiable.

Why Chainlink VRF?

Numbers derived from blockchain data alone (such as block hashes) can be influenced by miners or validators who can choose which blocks to publish. Chainlink VRF solves this by generating randomness off-chain and delivering it with a cryptographic proof that is checked on-chain before the result is accepted. Even Chainlink itself cannot manipulate the outcome.

How It Works

1. When a round closes, the contract sends a request to the Chainlink VRF service.
2. Within a few minutes, Chainlink delivers two random values, each with a cryptographic proof.
3. The contract verifies the proof on-chain. If it fails, the values are rejected.
4. If it passes, the six winning numbers and bonus number are derived from the values using a fair shuffle algorithm, and permanently recorded on-chain.

The VRF request and fulfilment always occur in **separate blocks**. This temporal separation ensures that no party — including validators — can observe the winning numbers and act on them before ticket sales close.

What Happens If VRF Is Unavailable?

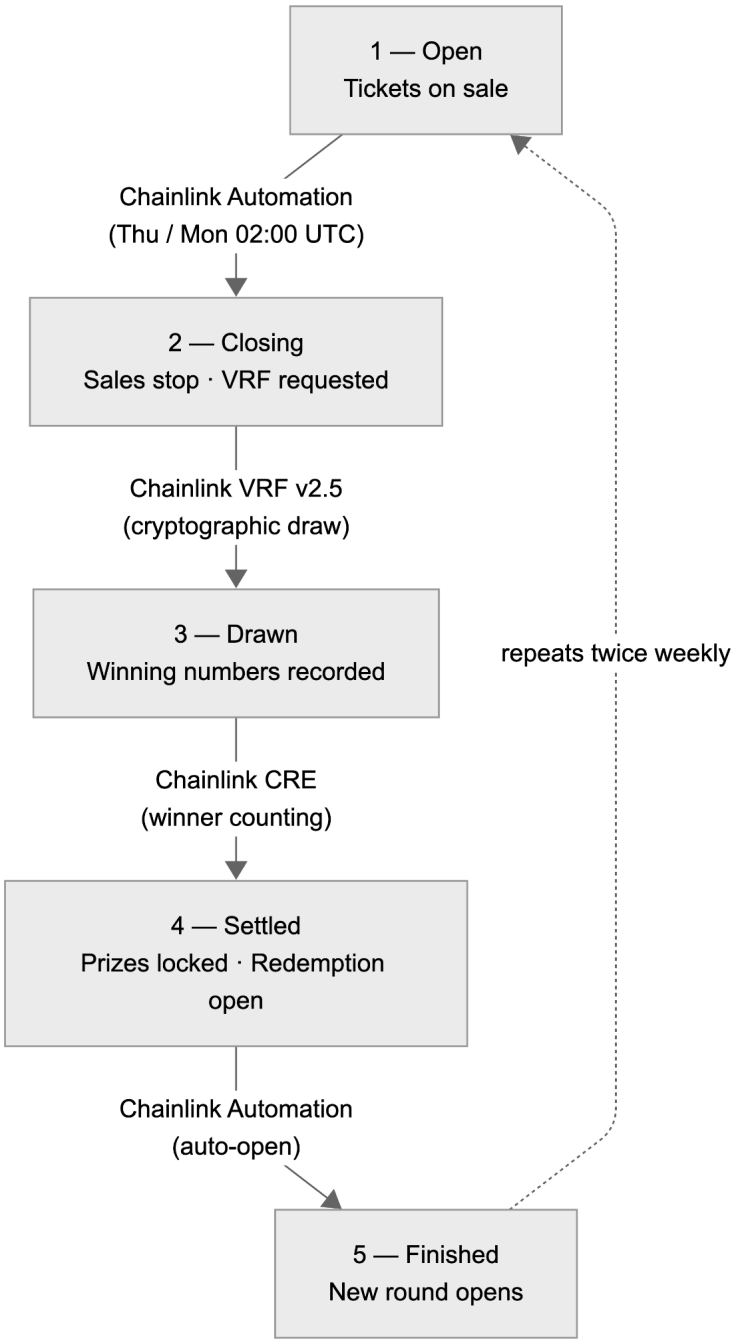
If Chainlink VRF does not respond — for example during a temporary outage — the protocol does not stall. The team can resubmit the randomness request to reset the waiting window. This re-request mechanism ensures the protocol never gets permanently stuck while maintaining the same VRF security guarantees — the team cannot choose, supply, or influence the winning numbers.

---

10. Automated Round Lifecycle

Once CyberLotto is deployed, rounds run continuously with no manual intervention required from the team.

Stage	What happens
1. Open	Tickets are on sale. Chainlink Automation monitors the clock.
2. Closing	At 02:00 UTC on Thursday or Monday, Automation closes the round and the contract requests randomness from Chainlink VRF.
3. Drawn	VRF delivers the winning numbers in a separate block. The Chainlink CRE node network begins counting winners.
4. Settled	CRE nodes agree on winner counts and submit them on-chain. Prize amounts are locked. Players can redeem.
5. Finished → Open	Chainlink Automation detects settlement and automatically opens the next round.



No owner transaction is required for any of these stage transitions during normal operation. The team retains manual override capability only as an emergency backup. The draw schedule is governed by a swappable `CyberLottoScheduler` contract — CLT holders can propose and vote to change the frequency or timing through DAO governance.

---

11. Security Model

Prize Pool Isolation

The prize pool and the operator fee are stored in completely separate balances. There is no function in the contract that allows the team to touch prize funds. Prizes flow out only when a winning ticket holder redeems their ticket. Anyone can add funds to the prize pool at any time.

One Redemption Per Ticket

When a player redeems a ticket, the contract marks it as claimed before any transfer is sent. This prevents any attempt to redeem the same ticket twice, even through re-entrant calls.

Randomness Cannot Be Manipulated

Chainlink VRF delivers a cryptographic proof alongside every result. The proof is checked on-chain before the numbers are accepted. The team cannot know the result before the round closes, alter it after the request is submitted, or reuse a result from a prior round. The VRF request and fulfilment are always processed in separate blocks, eliminating any window for front-running.

Winner Counts Cannot Be Gamed by One Party

Winner tallies are submitted by the Chainlink CRE network, which requires multiple independent nodes to reach the same answer before anything is submitted on-chain. The team's manual override path exists only for emergencies and is fully transparent — any manually submitted count can be independently verified using an on-chain audit function.

Prize Pool Solvency Check

Before prizes are locked in each round, the contract verifies that the pool contains enough USDC to cover all payouts. If it does not, the round cannot be settled until the pool is adequately funded. The protocol will never commit to paying out more than it holds.

Cross-Chain Message Integrity

Cross-chain messages are delivered by Chainlink CCIP, which provides finality verification and an independent risk management network. On top of CCIP's transport security, the Hub validates every inbound message against an owner-managed allowlist of chain selectors and Satellite addresses. Messages from unknown chains or unrecognised addresses are rejected. The Satellite similarly validates that all inbound messages originate from the expected hub chain and hub contract address.

Automatic Refunds on Failure

If a cross-chain purchase fails for any reason — the round is not active, the draws are invalid, or any other error — the Hub automatically sends the USDC back to the Satellite via Chainlink CCIP, which transfers it to the original buyer. No funds are lost or stuck.

---

12. Cross-Chain Ticket Purchasing

Why Cross-Chain Matters

The core CyberLotto contracts live on Base. Without cross-chain support, players on other EVM chains would need to manually bridge their USDC to Base, purchase tickets there, and bridge prizes back — a multi-step process with friction, gas costs, and bridge risk at every hop.

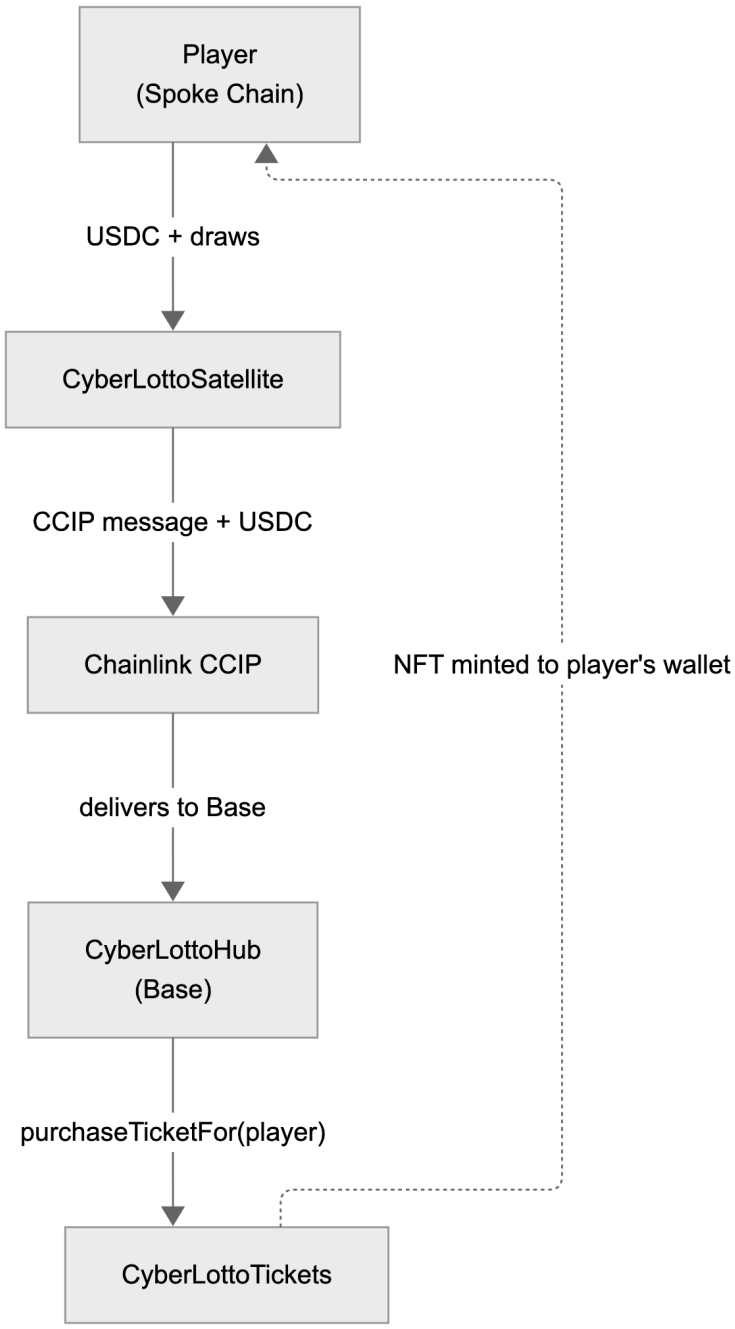
Chainlink CCIP (Cross-Chain Interoperability Protocol) eliminates this friction. CCIP provides a standardised, audited messaging and token transfer layer between EVM chains. Players interact with a local contract on their own chain, and the system handles the rest.

Hub-and-Spoke Architecture

CyberLotto uses a hub-and-spoke model for cross-chain participation:

- **Hub (CyberLottoHub)** — deployed on Base, the same chain as `CyberLottoTickets`. The Hub is the single point of contact between CCIP and the core lottery. It receives cross-chain messages, executes purchases on `CyberLottoTickets`, and sends refunds back when purchases fail.
- **Satellites (CyberLottoSatellite)** — one deployed per supported spoke chain. Each Satellite provides the user-facing `purchaseTicket` function and handles draw validation, USDC collection, and CCIP message construction.

This design keeps all lottery state — rounds, results, prize pool, and ticket NFTs — on a single chain, avoiding the complexity and inconsistency risks of duplicating state across networks.



How Cross-Chain Purchasing Works

When a player on a spoke chain wants to buy a ticket, the experience is a single transaction on their own chain. Behind the scenes, the following steps happen automatically:

1. The player calls `purchaseTicket(draws)` on the CyberLottoSatellite contract on their spoke chain.

2. The Satellite validates the draw selections locally — the same rules apply as on the main contract (exactly 6 numbers from 1–49 per draw).
3. The Satellite pulls USDC from the player (ticket cost plus the 4% fee).
4. A Chainlink CCIP message is constructed containing the player's address, draw selections, and the USDC transfer, then sent to the Hub on Base.
5. The Hub receives the message, approves `CyberLottoTickets` to pull the USDC, and calls `purchaseTicketFor(player, draws)`.
6. The ticket NFT is minted directly to the player's wallet address on Base.

From the player's perspective, they sign one transaction on their spoke chain and receive a ticket NFT on Base.

Refund Handling

If the purchase fails on the hub chain — for example, the round is not active, or the draws fail validation — the Hub does not simply discard the player's USDC. Instead, it automatically sends the USDC back to the originating Satellite via Chainlink CCIP. The Satellite receives the refund and the funds are returned. No manual intervention is needed and no funds are lost.

Satellite Allowlisting

The Hub maintains an allowlist of authorised Satellites, keyed by CCIP chain selector. Only messages from an allowlisted chain selector and matching contract address are accepted. The owner can add or remove Satellites at any time. This prevents unauthorised contracts from submitting fake purchase requests.

Fee Management

CCIP messages require a fee to cover cross-chain delivery. The Satellite pays for purchase messages using the spoke chain's native token (e.g. ETH), included by the player directly in their purchase transaction. The Hub pays for refund messages using LINK tokens, funded by the operator.

Each Satellite provides an `estimatePurchaseFee` function that returns the expected native token cost for a given purchase, so players can include the correct amount with their transaction. The owner can adjust gas limits, withdraw native tokens from Satellites, and withdraw LINK from the Hub.

Cross-Chain Scope

Cross-chain functionality is limited to **ticket purchasing only**. Ticket NFTs are minted directly to the player's wallet address on Base, meaning all post-purchase operations — including prize redemption, free ticket claims, and ticket burns for CLT — require the player to interact with the Base network. Players who purchase cross-chain should connect to Base to manage their tickets.

This design keeps all lottery state on a single chain, eliminating the consistency risks and attack surface that would come with distributing redemption logic across multiple networks.

---

13. DAO Governance

CyberLotto is governed by a fully on-chain DAO. CLT token holders propose and vote on protocol changes; approved actions execute through a **48-hour timelock** that gives the community time to review any change before it takes effect.

Parameter	**Value**
Voting delay after proposal	~1 day (7,200 blocks)
Voting period	~5 days (36,000 blocks)
Proposal threshold	1,000 CLT
Quorum	4% of CLT supply
Timelock delay	48 hours

What Governance Controls

- CLT minting roles and token distribution
- Protocol fee rate (capped at 10%)
- Treasury spending
- Round scheduler contract (determines draw frequency and timing — e.g. changing from twice-weekly to daily)
- Governor parameter updates

Governance does **not** control round mechanics, randomness, or winner counting — those are handled automatically by Chainlink.

Scheduler Governance

The `CyberLottoScheduler` contract determines when each round closes. It implements a standard interface that `CyberLottoTickets` queries to check whether the current round should end. The default scheduler closes rounds at 02:00 UTC on Thursdays and Mondays.

CLT holders can deploy an alternative scheduler contract — for example, one that runs daily draws or adjusts timing for different time zones — and submit a governance proposal to swap it in. If the proposal passes and clears the 48-hour timelock, the new scheduler takes effect

immediately. The main lottery contract does not need to be modified or redeployed; it simply calls the new scheduler's interface.

Revenue Sharing

CLT holders can stake their tokens in the **RevenueSharing** contract to earn a proportional share of protocol fee revenue. When the DAO treasury distributes fees, stakers claim their USDC rewards directly from the contract.

Revenue flow: ticket sales → protocol fee → DAO treasury → RevenueSharing contract → CLT stakers.

---

14. Technical Reference

Core Parameters

Parameter	**Value**
Number pool	1 – 49 (49 numbers)
Numbers per draw	6
Bonus number pool	Remaining 43 (not in main draw)
Ticket price per draw	5.20 USDC (5.00 pool + 0.20 fee)
Default fee rate	4% (max 10%, adjustable by governance)
Round schedule	Twice weekly — Thu & Mon 02:00 UTC (governance-changeable)
Payment token	USDC (6 decimals)
Home chain	Base
Ticket standard	ERC-721 (NFT with enumeration)
CLT hard cap	1,000,000,000 CLT
VRF random values per round	2
Jackpot seed reserve	10% of prize pool per round
Cross-chain protocol	Chainlink CCIP

Parameter	Value
Hub contract	CyberLottoHub (Base)
Satellite contract	CyberLottoSatellite (per spoke chain)
CCIP fee token	Native token (Satellite) / LINK (Hub)
Free ticket credit rate	1,000 credits per tier 5/6 win; 1,000 credits per free ticket
Scheduler interface	Swappable via DAO governance proposal

Winning Odds

Tier	Condition	Combinations	Odds (1 in …)
1	Match 6 of 6	1	13,983,816
2	Match 5 of 6	258	54,201
3	Match 4 of 6	13,545	1,032
4	Match 3 of 6	246,820	57
5	Match 2 of 6	1,851,150	7.6
6	Match 1 + bonus	1,147,686	12.2
—	No prize	10,724,356	1.3

Total combinations: C(49,6) = 13,983,816. The overall chance of winning any prize is approximately 23.2%.

CyberLotto — transparent, non-custodial, provably fair.

Built on Base · Powered by Chainlink · Multi-chain via CCIP · Governed by CLT holders