BCH BLAZE 2026

Lotry *on* XO

The lottery the organiser can't run away with.

Team: Nikhil PN & Hina Hanan

lotry-xo.exprmnts.fun

@X_HANDLE_PENDING

github.com/nikhil-pn/lotry-xo



The Story of Lotry

In 2025 we built **Lotry.fun on Base** at Base Batch India, where it was a **runner-up**. Tickets were tokens, a contract held the pot, and Chainlink VRF picked the winner.

But the pot sat in a contract with an owner, and the owner triggered the payout. Players had to trust that key.

On Bitcoin Cash a coin can carry its own rules. So for BLAZE we moved the core round there: **the pot is a coin with no key**, and the chain itself checks the draw, the payout and every refund.

2025 · BASE BATCH INDIA · RUNNER-UP

Lotry.fun on Base

ERC-20 tickets · owner-held pot · Chainlink VRF

NOV 2026 · BCH BLAZE

Lotry on XO

NFT tickets · keyless pot · commit-reveal checked on chain · refunds

Written during BLAZE. Live on Chipnet: 3 rounds, 15 transactions, every invitation file public.

Benefits of Lotry *on XO*

- **The organiser can never touch the pot**
  - no key, no admin path, no signature check at all
- **Tickets are real NFTs you hold**
  - numbered CashTokens in the player's own wallet
- **The winner is checked by the chain**
  - the covenant computes sha256(secret) mod tickets + 1
- **Refunds if the organiser vanishes**
  - every ticket pays back after the refund height
- **Sub-cent fees on Bitcoin Cash**
- **One reviewable template**
  - every rule in one file; 43 tests, 25+ attacks refused

BCH *Usage*

Every rule of the round runs in Bitcoin Cash script. Nothing off chain holds the money.

CashTokens: genesis + a minting NFT as state

Opening a round creates its own token category. The pot's minting NFT commitment is the round: ticket count, then the winner.

Covenant introspection

The pot checks its next self: same script, same category, value + price, count + 1, one immutable ticket out (`OP_OUTPUTVALUE`, `OP_UTXOTOKENCOMMITMENT`).

OP_CHECKLOCKTIMEVERIFY, after Faster Blocks

Draw and refund heights in lock heights, which now advance once every ten 1-minute blocks. We measured Chipnet's activation: block 332,451.

XO invitations, two parties

A sale is one transaction: the organiser adds the pot, the player adds coins and takes the ticket, each signs their own part.

THE DRAW PATH OF THE POT COVENANT

```
<drawHeight> OP_CHECKLOCKTIMEVERIFY OP_DROP
OP_DUP OP_SHA256 <secretHash> OP_EQUALVERIFY
potIsOpen                    // 4-byte ticket count
OP_BIN2NUM OP_DUP OP_0 OP_GREATERTHAN OP_VERIFY
OP_SWAP OP_SHA256 <4> OP_SPLIT OP_DROP
<0x00> OP_CAT OP_BIN2NUM
OP_SWAP OP_MOD OP_1ADD        // winner
OP_4 OP_NUM2BIN <0xd0> OP_CAT
OP_0 OP_OUTPUTTOKENCOMMITMENT OP_EQUALVERIFY
potCarriesOn                 // same script + NFT
OP_0 OP_OUTPUTVALUE OP_0 OP_UTXOVALUE
OP_NUMEQUALVERIFY            // keeps every sat
```

The Vision for *Lotry*

- **Buy a ticket from a browser wallet**
  - WizardConnect: connect, approve, hold the ticket
- **Buyer-supplied randomness**
  - mix in every buyer's input, so the organiser alone can't steer the draw
- **Recurring daily rounds**
  - a new pot every day, refunds always on
- **Mainnet after May 2027**
  - once Faster Blocks reaches mainnet (15 May 2027)



Thank *you!*

Nikhil PN & Hina Hanan

lotry-xo.exprmnts.fun github.com/nikhil-pn/lotry-xo

Before BLAZE: lotry.fun (Base, 2025) · github.com/exprmnts/Lotry_contract