Pot

Bounties that pay out, on Bitcoin Cash



Built by apeir · BCH BLAZE 2026, Mainnet track
+ Paytaca Decentralized Identity bounty

apeir.dk/online/pot github.com/apeirs/pot @apeirs

Bounty Pot!

Lock a bounty on chain. A named judge awards it.
If nobody wins by the deadline, the poster takes it back.

TRY IT IN 2 MINUTES, ON MAINNET

1. Open the page: the **BLAZE 2026 demo pot** holds 0.0005 BCH, read live.
2. **Connect wallet**: scan the WizardConnect QR with Paytaca or Selene.
   Or pay the pot's QR from any BCH wallet.
3. Add to the pot, or **Create a pot**, and sign in your wallet.
4. Your tx id appears, with an explorer link.

https://apeir.dk/online/pot/

github.com/apeirs/pot · mainnet award `d7f47d5e` · refund after deadline `50afa3db`

The Story of Pot

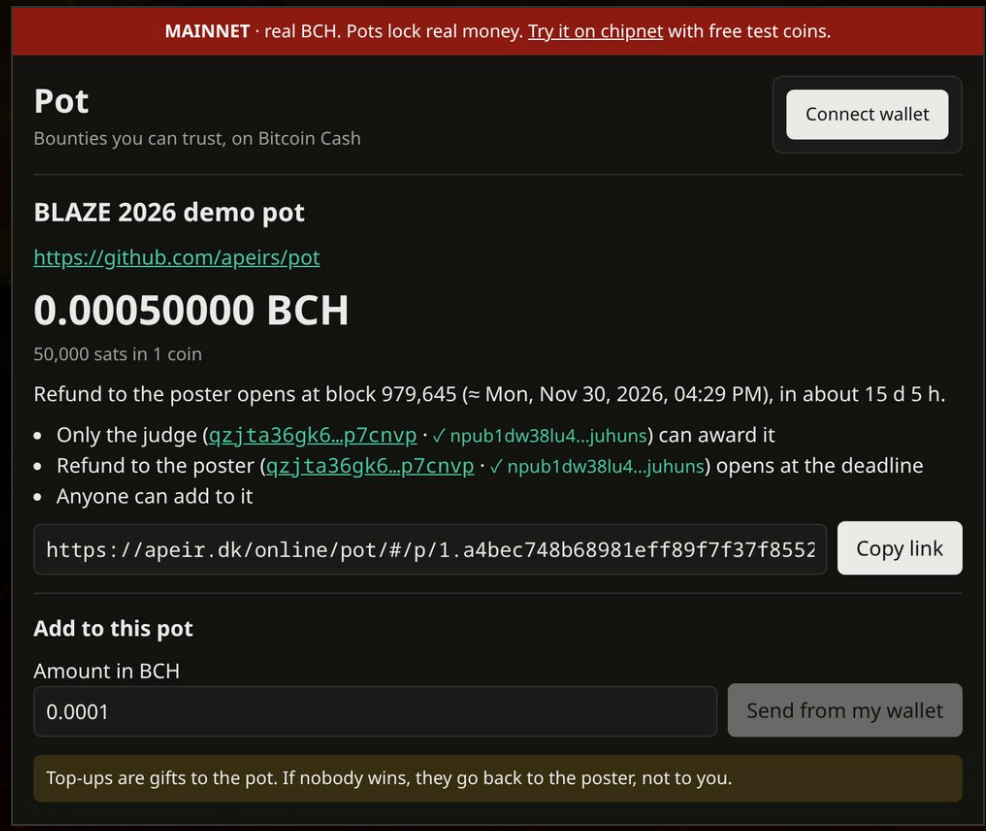
We are bounty hunters. We get paid after the work, if the poster pays.

We earn from bug bounties and paid code reviews. The work always comes first; the payment is a promise.

Most posters pay. Some never answer. A hunter can't tell beforehand which kind this one is.

What we wanted: the prize visibly locked before anyone starts, and payout rules that are code, not goodwill.

Bitcoin Cash can do this today in a covenant, with sub-cent fees and wallets people already use. So we built it.



The live demo pot on mainnet: 0.0005 BCH locked until block 979,645, judge and poster shown with their verified npub.

Benefits of Pot

Each line is enforced by the contract or done by the live page. Every contract rule is tried by a test in `npm test`.

- **Locked before work starts**
  Anyone can check a pot's balance on chain before spending an hour on it.
- **No early pull-back**
  Refund opens only at the deadline block, and only to the poster's own address.
- **A judge with a name**
  Only the judge key can award. It can't pay the poster's or the judge's own key address, and the fee is capped at 5,000 sats.
- **Anyone can add to it**
  Sponsors top up with a plain payment. The award sweeps every top-up in one transaction.
- **No backend, no account**
  One static page, your own wallet over WizardConnect, and the chain. Nothing to sign up for.
- **Pay a winner by Nostr name**
  Paste an npub: the award goes to the BCH address that npub provably bound to.



BCH Usage

One CashScript covenant: `Pot(posterPkh, judgePk, deadline, maxFee, salt)`

SPEND PATH	WHO SIGNS	WHAT THE CONTRACT ENFORCES
`top-up`	**anyone**	nothing: a plain payment to the pot address (title in a POT1 OP_RETURN)
`award(judgeSig)`	**judge**	one output, not to the poster's or the judge's P2PKH; every input is this pot; output ≥ total − maxFee
`refund(posterPk, sig)`	**poster**	only from the deadline block on (`tx.time`); only to the poster's own address; same sweep and fee cap

MAINNET, SIGNED IN THE WALLET OVER WIZARDCONNECT

Paytaca

create A	`8457e87d`
top-up A	`48dcebb3`
award A, 2 coins	`d7f47d5e`
create B	`9d17abd3`
refund B	`50afa3db`
open pot C	`8223691c`

Selene

create	`5e14240d`
award as judge	`335210ab`

Nostr binding

npub ↔ address	`adf8a87d`

WALLETS TRIED (MAINNET)

WALLET	CREATE	TOP-UP	AWARD	REFUND	ID PROOF
Paytaca 0.27.5	**yes**	**yes**	**yes**	**yes**	**yes**
Selene web	**yes**	not yet	**yes**	not yet	not yet

Award and refund: the wallet signs the CashScript contract input itself (`inputPaths`).

Self-audit in the README: one row per rule (15 `requires`), the attack it stops and the test that tries it; **103 tests** with `npm test`.

The Vision for Pot

Goal: BCH projects post their bounties as Pots, and hunters pick work by locked balance, not by reputation alone.

- **Registered entries**
  Each hunter's submission is committed on chain as a CashToken, and an award can pay only a registered entry.
- **Panels and splits**
  2-of-3 judge pots for DAOs, and one award paid out to several winners.
- **A bounty board**
  One page that lists every Pot on chain, rebuilt from the chain, with no server.
- **Sign in with Nostr**
  A challenge signed by the npub, checked against its BCH binding: "signed in as npub · bch:address".



THANK YOU!



Pot: try it at apeir.dk/online/pot

github.com/apeirs/pot · pre-hackathon prep: public gist · @apeirs

EMBER2026 / TokenHunt: `bitcoincash:zrk8th0g30cn28um7apj85un4l9vvd37lyf6j3l26f`