HOW IT WORKS

The house rules in full: the ticket, the proof, what the chain records, results, fees, refunds and limits.

`figures read 2026-11-25 05:16 UTC`

01 WHAT DARKHORSE IS

DARKHORSE is a pari-mutuel betting market on Solana, paid in USDC. A person buys tickets of one fixed value, 5.00 USDC each, with a wallet. Each ticket is then placed on one side of a market with a zero-knowledge proof instead of a wallet signature, and a relay sends that transaction, so no wallet of the bettor appears on the placement.

Every market shows, on chain and on this site, how many tickets sit on each side. The two sides share the pot. The project puts no money into any pot and takes no side: the project places no bets. That is the project's commitment; the chain shows the tickets on each side, not who placed them.

There are two kinds of market: a SOL price round that opens every 30 minutes and settles from an on-chain price, and event markets that follow a named public prediction market.

02 A TICKET, THE BOOTH, THE BOARD, THE STUB



TICKET

One unit of a fixed value, 5.00 USDC, usable in any market. A wallet pays the program for each ticket it buys. For each ticket the browser makes two secret values and sends only their Poseidon hash; the program adds that hash as a leaf of one on-chain Merkle tree. A ticket belongs to no market until it is placed.



THE BOOTH

Where a ticket is placed: a proof, no wallet. The browser proves it holds an unplaced ticket in the tree and names a market and a side. The program checks the proof, marks the ticket used, adds one to that side of the market's board and adds a stub to the tree.



THE BOARD



THE STUB

Per market, the ticket count on each side. It is held in the market's account on chain and anyone can read it.

The bettor's half of a placed ticket. It pays if its side wins. Its secrets live only in the bettor's browser; the program records the stub's leaf, tagged with the market and side, in the tree.

03 WHAT THE PROOF PROVES

Every placement, claim and refund carries one Groth16 proof from one circuit. The proof shows that the sender knows the two secret values of one leaf in the program's Merkle tree, without saying which leaf.

- **The leaf exists.** The leaf is in the tree at a recent root the program has stored.
- **It is used once.** The proof yields a nullifier computed from the leaf's secret and position. The program records every nullifier and refuses one it has seen before, so a ticket is placed once and a stub is claimed once.
- **It is the right kind of leaf.** A placement and a ticket refund need an unplaced ticket. A claim needs a stub of the winning side of that market. A void refund needs a stub of that void market.
- **The terms are bound.** The proof is bound to the market, the side, the new stub, the receiving wallet, the relay and the relay fee. The program recomputes these from the transaction itself, so none of them can be changed after the proof is made.

Anyone can check a placement's proof again on /proof.

04 WHAT THE CHAIN RECORDS, AND WHAT IT DOES NOT

WHAT THE CHAIN RECORDS

- Which wallet bought how many tickets, and when.
- For each market, the ticket count on each side and the time of each placement.
- The wallet and amount of every claim and every refund.

WHAT THE CHAIN DOES NOT RECORD

- Which ticket was placed in which market, or on which side.
- Whose a losing ticket was.

05 TWO WAYS A BET CAN STILL BE GUESSED

- **Time and count.** If a wallet buys a number of tickets and the same number of tickets lands on one side of a market right after, the two can be linked by their timing and count. The app suggests buying tickets ahead of time, so purchases and placements are apart.
- **Claim to the buying wallet.** If a win is claimed to the wallet that bought the tickets, that wallet is then known to have won in that market. The app lets a claim go to any wallet the bettor chooses.

The crowd a bet sits in is the number of wallets that have bought tickets. That number is shown on the site where tickets are placed.

06 RESULTS

SOL ROUNDS

- A new round starts every 30 minutes, at :00 and :30 UTC.
- A round is open for placements for 30 minutes, then running for 30 minutes.
- The price comes from one deep SOL/USDC pool on Solana: the Orca Whirlpool `Czfq3xZZDmsdGdUyrNLtRhGc47cXcZtLG4crryfu44zE` (wSOL/USDC, 0.04% fee tier), pinned in the program.
- For the 90 seconds after the lock time, and again for the 90 seconds after the end time, the round keeper reads the pool once in each 6-second slot of time: 15 readings per window. A reading takes the pool's own on-chain state at that moment; the keeper cannot supply a number and cannot choose the winner. By taking fewer than 12 readings in a window it can only make the round void.
- The project's keeper is set to take each reading at a random moment inside its 6 seconds, so the moment cannot be known in advance; this is how the keeper runs, not a rule the program enforces. A reading is refused when anything other than this program's own instruction is in the same transaction, and when the pool's liquidity is below a floor.
- The lock price is the lower median of the readings after the lock time; the end price is the lower median of the readings after the end time. UP wins if the end price is higher, DOWN wins if it is lower.
- A window needs at least 12 of its 15 readings. If the keeper takes fewer than 12 in a window, the round is void and every ticket in it is refunded at 5.00 USDC, with no market fee (a refund sent through the relay pays the relay fee). The ledger on /proof shows, for

every SOL round, how many readings each window got and whether it settled or was void.

- Anyone can call the settling once a window has ended. A result lands about 2 minutes after the round's end time.
- An equal lock and end price (a tie) makes the round void.

EVENT MARKETS

- An event market follows a named public prediction market, linked on the market's page.
- Its result is posted by the project's result key, following the result of that named public market.
- A posted result can be corrected for one hour. Claims open when that window ends.

On a result, the payout of one winning ticket is fixed at once: the pot minus the fee, divided by the number of winning tickets. A market with one side empty, a tie on a SOL round, or a market voided before its result is void.

07 THE RELAY

The relay sends placements, claims and refunds for the bettor and pays the network fee, so the bettor's wallet does not appear as the fee payer. It runs behind the site's proxy. It sees a visitor's network address and keeps no record of it.

The relay can refuse to send a transaction. It cannot change the market, the side, the receiving wallet or its own fee, because the proof binds them, and the program caps the relay fee at the configured value.

Anyone can send their own placement, claim or refund directly, without the relay. The sending wallet then shows as the fee payer.

08 HOW THE PROVING SETUP WAS MADE

The proving key and the verifying key were made in two phases. Phase 1 is a public Powers of Tau ceremony, taken from its published file (powersOfTau28_hez_final). Phase 2, specific to this circuit, was run by the project alone: the project was the only contributor. The transcript of the setup is published on /proof.

09 FEES

- A settled pot pays a fee of 3%: 2% to the burn bucket, which buys and burns $DARKHORSE, and 1% to operations (the relay and running costs).
- A void market pays no fee.
- A relayed claim or refund pays the relay 0.05 USDC out of the amount paid. A relayed placement is free to the bettor.
- A transaction sent directly pays only the Solana network fee.

FIGURES IN FORCE — read 2026-11-25 05:16 UTC

Ticket price	**5.00** USDC
Fee on a settled pot	**3%** 2% burn bucket, 1% operations
Relay fee	**0.05** USDC on a relayed claim or refund; a placement is free
SOL round open	**30** min
SOL round running	**30** min
Correction window	**1** h event markets; claims open after it
Refund of an unplaced ticket	**24** h after it was bought
Pot cap, SOL round	**500** tickets
Pot cap, event market	**20,000** tickets

10 REFUNDS

- An unplaced ticket can be refunded at 5.00 USDC to any wallet, from 24 hours after it was bought.
- A stub of a void market can be refunded at 5.00 USDC at once.
- Both use the same kind of proof as a claim.

11 POT CAPS

- A SOL round holds up to 500 tickets.
- An event market holds up to 20,000 tickets.
- These are the caps at launch. The admin can raise them.

12 BLOCKED REGIONS

The app and the relay do not accept actions from visitors in these regions (the country comes from the proxy's header). Pages stay readable from every region.

This list is a setting of the site and the relay. The program itself cannot block anyone: a transaction sent directly to the program is checked only by the program's own rules.

IRAN (IR) SYRIA (SY) CUBA (CU) NORTH KOREA (KP) ARGENTINA (AR) AUSTRALIA (AU)
BELARUS (BY) BELGIUM (BE) BURUNDI (BI) BRAZIL (BR) CENTRAL AFRICAN REPUBLIC (CF)
CONGO - KINSHASA (CD) ETHIOPIA (ET) FRANCE (FR) GERMANY (DE) IRAQ (IQ) ITALY (IT)
LEBANON (LB) LIBYA (LY) MYANMAR (BURMA) (MM) NEW ZEALAND (NZ) NICARAGUA (NI)
POLAND (PL) RUSSIA (RU) SINGAPORE (SG) SOMALIA (SO) SLOVAKIA (SK) SLOVENIA (SI)
SOUTH SUDAN (SS) SUDAN (SD) TAIWAN (TW) THAILAND (TH) UNITED KINGDOM (GB)
UNITED STATES (US) U.S. OUTLYING ISLANDS (UM) VENEZUELA (VE) YEMEN (YE)
ZIMBABWE (ZW) IRELAND (IE) JAPAN (JP) NETHERLANDS (NL) SOUTH KOREA (KR)

Subdivisions, refused when the proxy reports one

UA-43 UA-14 UA-09 CA-BC CA-ON CA-AB CA-QC

13 OPEN SOURCE

The browser makes its proofs with the prover library snarkjs, which is licensed GPL-3.0. It is served as its own file, unmodified, and not compiled into the site's code. Its source: github.com/iden3/snarkjs.