

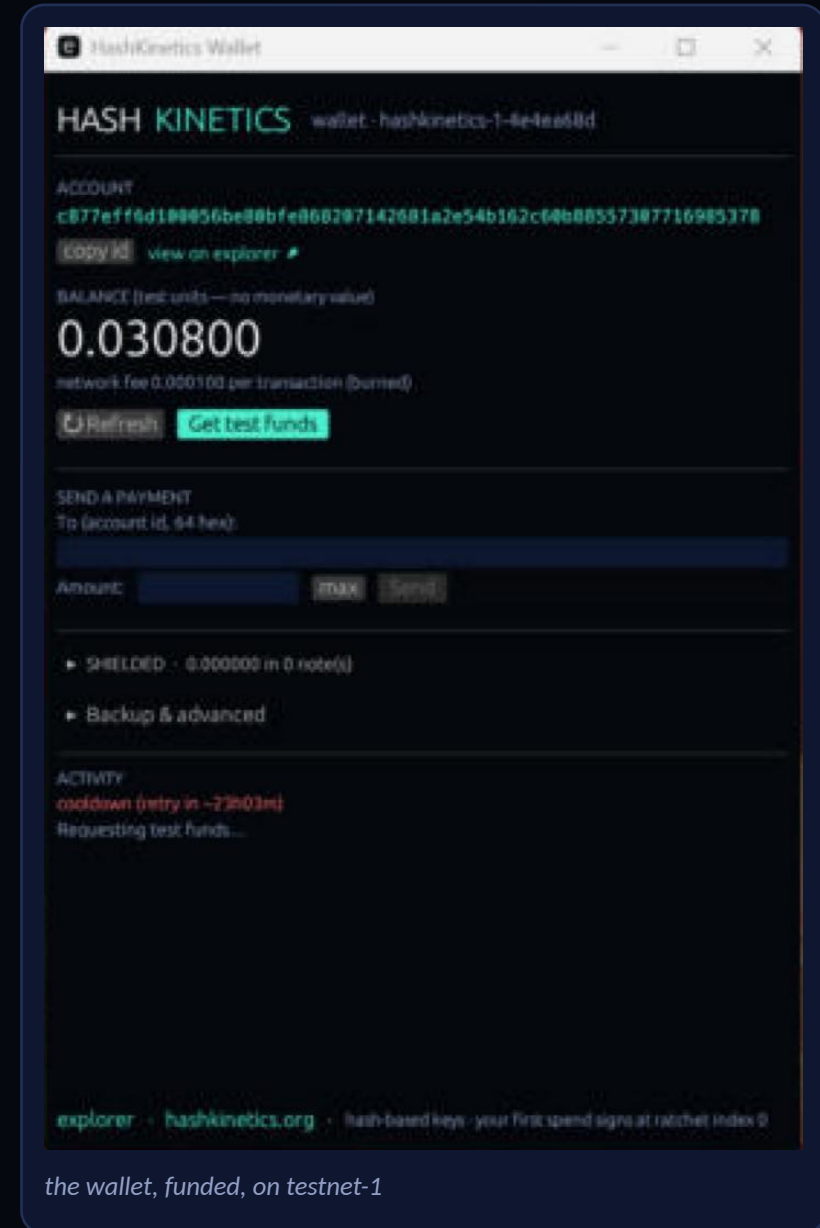
HASHKINETICS

Wallet user guide

What to click first, how to get test funds, how to pay, how to hide money in the shielded pool, how to show it again, how to pay someone privately, and how to prove one payment to an auditor without revealing anything else.

HashKinetics-Wallet.exe v0.13.0 · network testnet-1 (hashkinetics-1-4e4ea68d) · every screenshot in this deck is the real app on the live chain, 2026-09-02

Test units only — nothing in this wallet has monetary value. Nothing is for sale.



the wallet, funded, on testnet-1

Before you start

DOWNLOAD

github.com/hashkinetics/hashkinetics/releases → HashKinetics-Wallet.exe (v0.13.0). Check the sha256 shown on the release page against Get-FileHash in PowerShell. It is an unsigned testnet build: Windows SmartScreen will warn — “More info → Run anyway”.

WHAT IT IS

A native Windows app (no browser, no install). Your keys are created on your machine and never leave it. The faucet and the chain only ever see a commitment — never a secret.

THE NETWORK

testnet-1 — a public test chain. Balances are test units with no monetary value. Every transaction pays a flat network fee of 0.000100 that is burned; the wallet shows it and keeps it back for you.

ONE WALLET PER MACHINE

Files live in `C:\Users\<you>\.hashkinetics\` — `account.json` (your seed) and, once you use the shielded pool, `shield.json`. Back both up. Delete the folder to start over (funds stay with the old seed).

1

First launch — create your wallet

WHAT TO CLICK

- Double-click HashKinetics-Wallet.exe. The first screen says “Get on the chain in one click.”
- Click the cyan “Create my wallet” button. That's it — a post-quantum keychain is generated locally and saved to account.json.
- Restoring on a new machine instead? Open “Restore from a seed”, paste the 64-hex seed from your backed-up account.json, click Restore. The chain's own nonce is adopted automatically.
- Nothing is sent anywhere until you ask for funds.

WHAT YOU'LL SEE

The activity log says “Wallet created. Your keys never leave this machine.” and shows your account id (64 hex). The balance reads “not on-chain yet” — the account exists on this machine but not on the chain until the faucet creates it.

HASHKINETICS wallet • hashkinetics-1-4e4ea68d

Get on the chain in one click.

This creates a post-quantum keychain on YOUR machine. Nothing is sent anywhere until you ask for funds.

Create my wallet

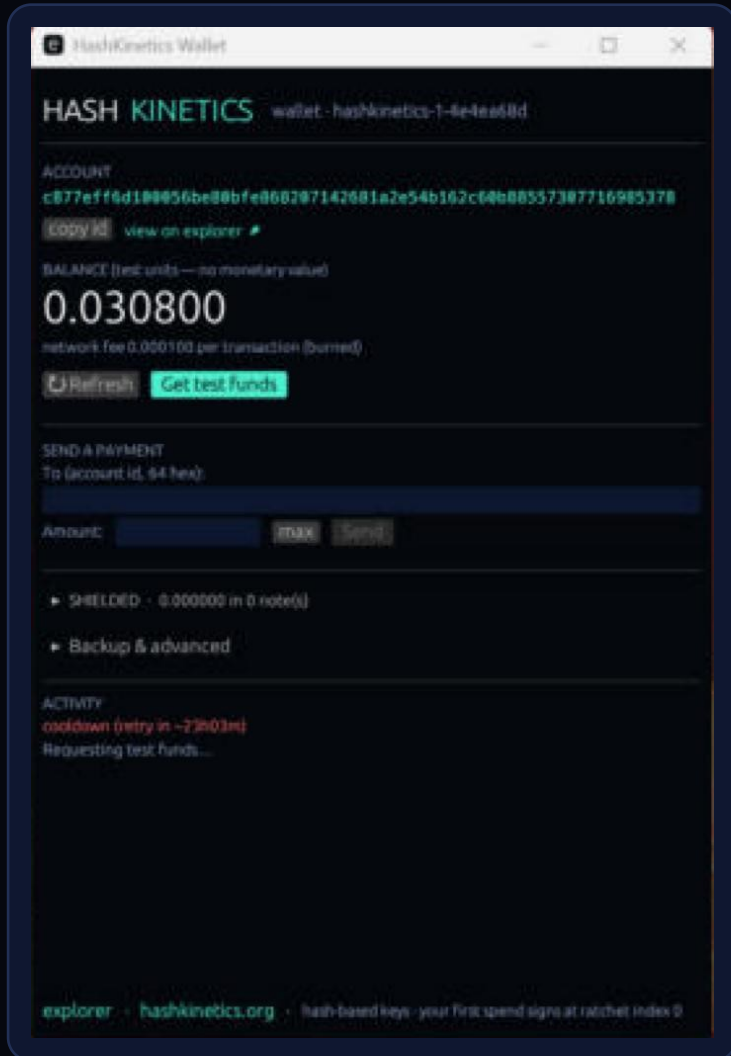
► Restore from a seed

Paste the 64-hex seed from a backed-up account.json:

Restore

illustration of the first-launch screen (an existing wallet on this machine was kept for the rest of the guide)

The main screen — what everything is



- 1 Network** — the chain id this wallet is talking to (hashkinetics-1-4e4ea68d = testnet-1). If it says “connecting...”, check your internet.
- 2 Account** — your public account id — the thing people pay TO. “copy id” copies it; “view on explorer” opens your history on hashkinetics.org/explorer.
- 3 Balance** — transparent (visible) balance in test units, and the network fee line: 0.000100 per transaction, burned.
- 4 Refresh / Get test funds** — Refresh re-reads the chain. Get test funds asks the faucet to create + fund your account (0.1 per day per IP).
- 5 Send a payment** — paste an account id, type an amount (or click max), Send.
- 6 SHIELDED** — the private pool: hide, show, pay privately, scan, disclose. Collapsed until you open it.
- 7 Backup & advanced** — your seed (copy it, keep it safe), the auth commit the web faucet asks for, the wallet file path.
- 8 Activity** — every step of every operation, newest first; “view ↗” opens the transaction on the explorer.

2

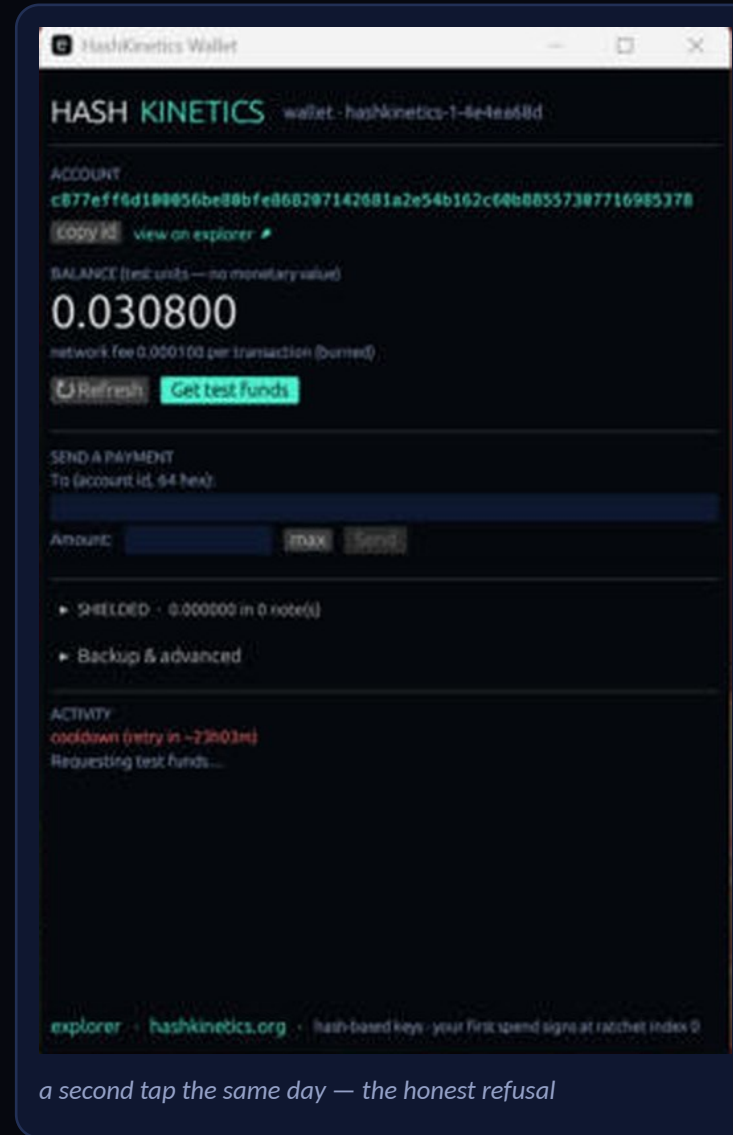
Get test funds (the faucet)

WHAT TO CLICK

- Click the cyan “Get test funds” button.
- First time: the faucet CREATES your account on-chain and funds it with 0.100000 — one real consensus transaction. Later taps top it up.
- Wait ~3 seconds; the balance refreshes by itself. Click ↻ Refresh any time.
- Limit: one drip per IP address per day. A second tap shows “cooldown (retry in ~23h)” — that is normal.

WHAT YOU'LL SEE

“Faucet dripped 100000 micro — tx ...” with a “view ↗” link to the transaction, then your balance: 0.100000. If the faucet is busy the activity says so; nothing is lost, just tap again later.



3

Send a payment (transparent)

WHAT TO CLICK

- Paste the recipient's account id (64 hex) into “To”. Ask them to click “copy id” in their wallet and send it to you.
- Type the amount, e.g. 0.005 — or click “max”, which fills balance minus the network fee.
- Read the preview: “= 5000 micro + 100 fee”. If it says “exceeds balance + fee” the Send button stays grey.
- Click Send. The wallet signs with your one-time hash-based key, submits, and waits for the receipt.

WHAT YOU'LL SEE

“Sending 0.005000 to eb2003d6...” then “Paid ✓ tx 194d4a0e... (ok: 1 event(s)) view ↗”. Balance drops by amount + 0.000100. A refusal never costs money — the wallet rolls its key index back and tells you why.



“max” = balance – fee, with the micro preview



amount typed; preview shows the fee on top



the receipt — click “view ↗” to open it on the explorer

4

Back up your keys (once, now)

WHAT TO CLICK

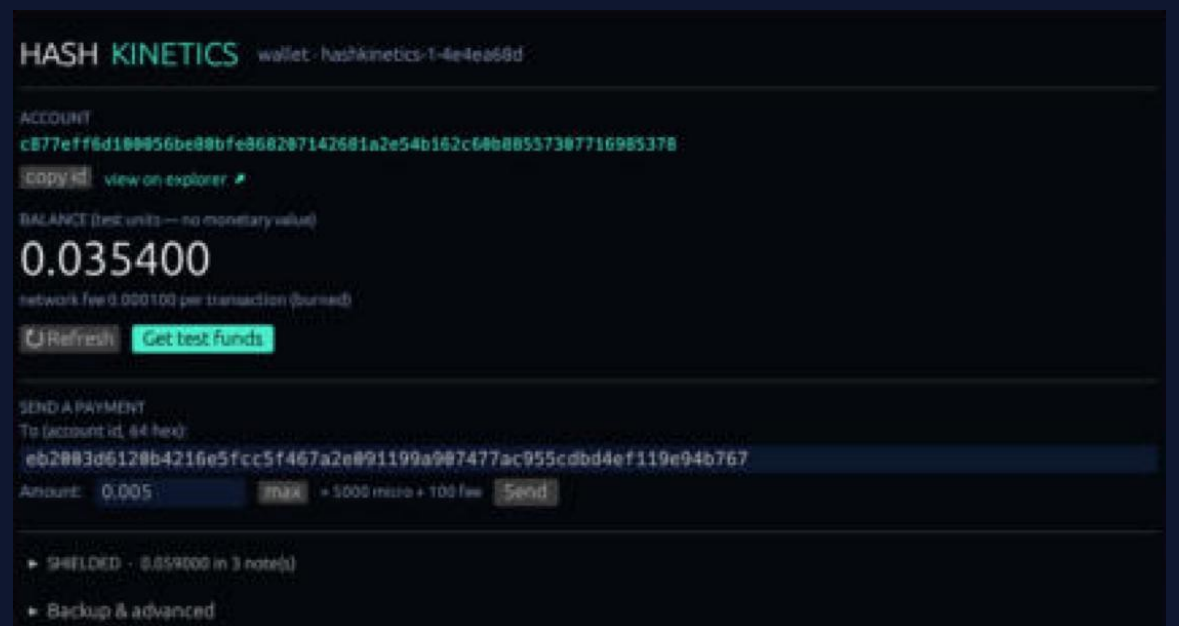
- Open “Backup & advanced”.
- Click “copy seed” and paste it somewhere safe and offline (a password manager). The seed IS the account: anyone holding it can spend.
- Note the wallet file path. account.json = transparent keys. shield.json (appears after your first shielded operation) = shielded keys + one-time counters. Back up BOTH.
- The “Auth commit” line is what the web faucet at hashkinetics.org/faucet asks for if you prefer the browser — it is public, not a secret.

WHAT YOU'LL SEE

A gold warning: “⚠ The seed IS the account. Back it up; never share it.”
Restoring later: fresh install → “Restore from a seed” → paste → the chain's nonce is adopted automatically; copy shield.json back into the folder to recover shielded notes.



Backup & advanced, expanded



the account header — “copy id” for receiving, “view on explorer” for history

The shielded pool — hide, show, pay privately

Money in the pool is held as notes. The chain stores only a commitment for each note and a nullifier when one is spent — never amounts, never who paid whom. Every shielded operation is a STARK proof made on the public prover (prover.hashkinetics.org), about a second each, and the wallet waits for the on-chain receipt like any other payment.

Shield → **pool** hide: moves an amount from your visible balance into a fresh note only you can find.

Pool → **me** show: spends one note back to your visible balance; the leftover becomes a new hidden change note.

Pay shielded pay someone privately to their stealth address (hkaddr:...) with an optional memo.

Scan pool finds every note that belongs to you (all epochs) and marks which are spent.

disclose writes a one-time package proving ONE received payment — for an auditor or a court — and nothing else.



the SHIELDED panel, opened, with one hidden note

WHAT THE CHAIN SEES

The explorer shows the pool as: total shielded \$0.06, commitments 6, nullifiers 2 — and the sentence “What you are NOT seeing: who paid whom, how much, which note was spent.” There is no master view key, structurally. The only window into a payment is a disclosure package its holder chooses to write.

5

Hide money: Shield → pool

WHAT TO CLICK

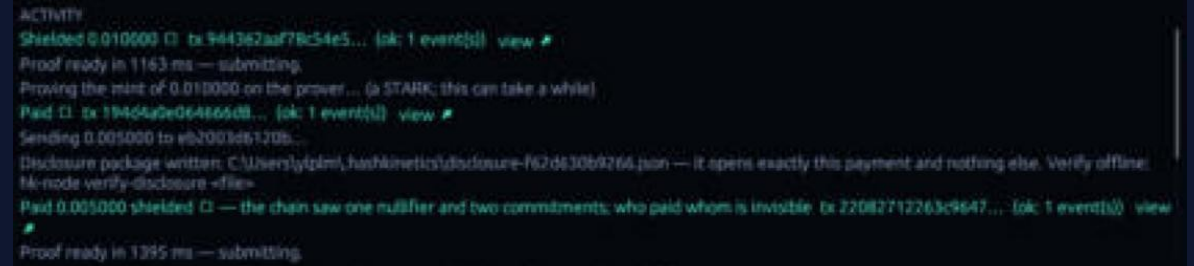
- Open the SHIELDED section (click its header).
- Type an amount in the “Shield” box, e.g. 0.01. It must fit in your visible balance together with the 0.000100 fee.
- Click “Shield → pool”.
- Wait: “Proving the mint of 0.010000 on the prover... (a STARK; this can take a while)” → “Proof ready in 1163 ms — submitting.”

WHAT YOU'LL SEE

“Shielded 0.010000 ✓ tx 944362aa... view ↗”. Your visible balance drops by 0.010100; the SHIELDED header now counts one more note. On the explorer the transaction shows a commitment — no amount.



amount typed into the Shield box



the activity log: shield proved and confirmed (top lines)

6

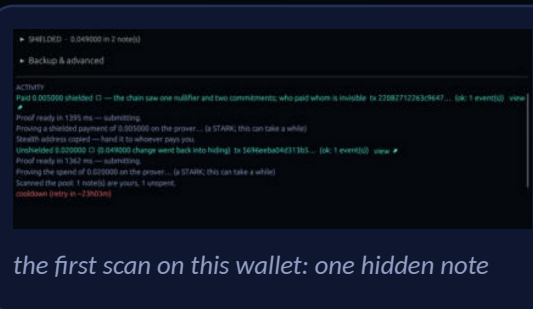
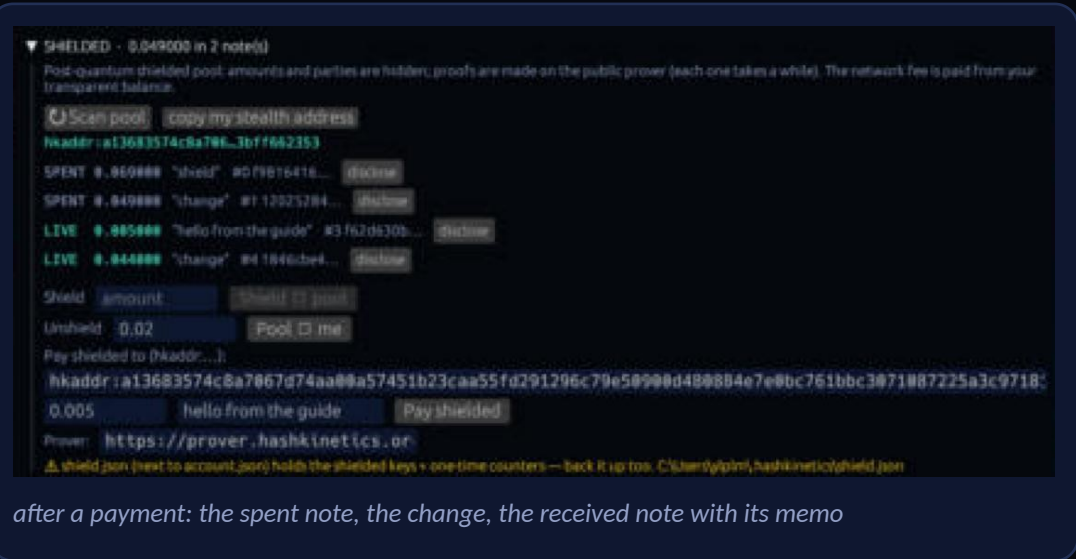
See what you own: Scan pool

WHAT TO CLICK

- Click “🔍 Scan pool”. The wallet trial-decrypts every note in the pool with your keys — only yours open.
- Each note shows LIVE (spendable) or SPENT, its amount, its memo, its position (#) and commitment.
- The header sums your LIVE notes: “SHIELDED · 0.059000 in 3 note(s)”.
- Click “copy my stealth address” to get the hkaddr:... string other people pay you at. Share it freely — it reveals nothing.

WHAT YOU'LL SEE

Your stealth address under the buttons, then the note list. A note you received carries the sender's memo (“hello from the guide”). Notes you spent stay listed as SPENT so your history is complete.



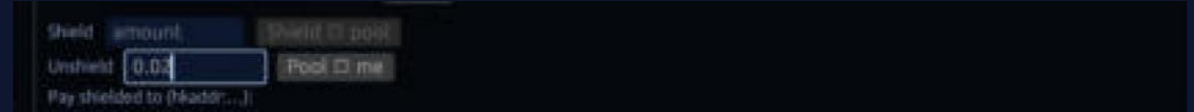
7 Show money again: Pool → me

WHAT TO CLICK

- Type the amount you want back in the visible balance in the “Unshield” box, e.g. 0.02.
- Click “Pool → me”. One hidden note is spent (the smallest one that covers the amount); the difference is re-hidden as a change note automatically.
- The 0.000100 fee is paid from your VISIBLE balance — keep a little there, or the wallet tells you to top up first.
- Wait for the proof (≈1.4 s) and the receipt.

WHAT YOU'LL SEE

“Unshielded 0.020000 ✓ (0.049000 change went back into hiding) tx 5696eeba... view ↗”. Visible balance up by 0.02 minus the fee; the scan now shows the old note SPENT and a new LIVE change note.



amount in the Unshield box



proving on the public prover — 1.36 s



the receipt, with the change amount

8 Pay someone privately: Pay shielded

WHAT TO CLICK

- Ask the recipient for their stealth address (they click “copy my stealth address”). Paste it into “Pay shielded to (hkaddr:...)”.
- Type the amount and, if you like, a memo — the memo travels encrypted inside the note; only the recipient can read it.
- Click “Pay shielded”. One of your notes is spent; the recipient gets a new note; your change is re-hidden.
- Fee: 0.000100 from your visible balance, as always.

WHAT YOU'LL SEE

“Paid 0.005000 shielded ✓ — the chain saw one nullifier and two commitments; who paid whom is invisible tx 22082712... view ↗”. The recipient sees nothing until they Scan — then the note appears with your memo.



recipient address, amount, memo



proof (1.4 s) and the receipt

9

Receive privately (and read the memo)

WHAT TO CLICK

- Give the payer your stealth address (“copy my stealth address” → paste in a message to them).
- When they say it's sent, click “🔄 Scan pool”.
- That's all. There is nothing to approve and nothing arrives in your visible balance — it lands as a hidden note.
- To spend it visibly later, use “Pool → me”; to pay it onward privately, use “Pay shielded”.

WHAT YOU'LL SEE

A new LIVE note with the amount and the memo, e.g. LIVE 0.005000 “hello from the guide”. The explorer, meanwhile, shows only a new commitment — your address, the amount and the memo are not on the chain.

The screenshot shows the HashKinetics Wallet interface. At the top, it displays the account ID: `hashkinetics-1-4e4ea68d`. Below this, the account address is shown: `c877e7fed100956be88bfe868287142681a2e54b162c60b8855738716985378`. The balance is `0.050600` units, with a network fee of `0.000100` per transaction. There are buttons for "Refresh" and "Get test funds".

The "SEND A PAYMENT" section shows a "To (account id, 64 hex)" field and an "Amount" field with "max" and "send" buttons.

The transaction history shows a "SHIELDED" transaction of `0.049000` in 2 notes. It includes a "Scan pool" button and a "copy my stealth address" button. The stealth address is `hkaddr:a13683574c8a7067d74aa0a57451b23caa55fd291296c79e50900d480884e7e0bc761bbc3071087225a3c9718`. The transaction details show two "LIVE" notes: one for `0.005000` with memo "hello from the guide" and another for `0.044000` with memo "change". There are buttons for "disclose" and "pay shielded".

The "ACTIVITY" section shows a "Disclosure package written" message and a "Paid 0.005000 shielded" transaction. It also shows a "Proof ready" message and a "Unshielded" transaction.

At the bottom, there is a link to the explorer: `explorer: hashkinetics.org`.

the whole wallet after a private payment to itself: 2 LIVE notes, one carrying the memo

10 Prove one payment: disclose

WHAT TO CLICK

- In the note list, click “disclose” next to the note you want to prove (a note you RECEIVED).
- The wallet writes a JSON package next to your wallet files: disclosure-<commitment>.json.
- Hand that file to the auditor. They verify it offline with the node tool: `hk-node verify-disclosure <file>`.
- The package opens exactly this payment — amount, memo, position in the pool — and nothing else: no spend authority, no other notes, no future visibility.

WHAT YOU'LL SEE

“Disclosure package written: C:\Users\<>you>\.hashkinetics\disclosure-f62d630b9266.json — it opens exactly this payment and nothing else.” This is the lawful-access design of the chain: scoped, holder-initiated, offline-verifiable. There is no master key to compel.

```
ACTIVITY
Shielded 0.010000  tx 944362aaf78c54e5... (ok: 1 event(s)) view #
Proof ready in 1163 ms — submitting.
Proving the mint of 0.010000 on the prover... (a STARK; this can take a while)
Paid  tx 19464a0e064866d8... (ok: 1 event(s)) view #
Sending 0.005000 to eb2003d6120b...
Disclosure package written: C:\Users\tylpmi\hashkinetics\disclosure-f62d630b9266.json — it opens exactly this payment and nothing else. Verify offline:
hk-node verify-disclosure <file>
Paid 0.005000 shielded  tx 22082712263c9647... (ok: 1 event(s)) view #
Proof ready in 1395 ms — submitting.
```

activity log with the disclosure line (third entry)

```
▼ SHIELDED - 0.049000 in 2 note(s)
Post-quantum shielded pool: amounts and parties are hidden; proofs are made on the public prover (each one takes a while). The network fee is paid from your transparent balance.
Scan pool copy my stealth address
hkaddr: a13683574c8a706...3b7f662353
SPENT 0.009000 "shield" #0 f9b1641e... disclose
SPENT 0.049000 "change" #1 12925284... disclose
LIVE 0.005000 "hello from the guide" #3 f62d630b... disclose
LIVE 0.044000 "change" #4 1846cbe4... disclose
Shield amount shield to pool
Unshield 0.02 Pool  me
Pay shielded to (hkaddr...):
hkaddr: a13683574c8a7067d74aa00a57451b23caa55fd291296c79e58990d480884e7e0bc761bbc3071087225a3c9718
0.005 hello from the guide Pay shielded
Prover: https://prover.hashkinetics.org
▲ shield.json (next to account.json) holds the shielded keys + one-time counters — back it up too. C:\Users\tylpmi\hashkinetics\shield.json
```

the “disclose” button sits on every note

Fees, refusals and the “max” button

EVERY TRANSACTION PAYS 0.000100

Transparent sends, shields, unshields and private payments all pay the same flat network fee. It is burned — nobody receives it. On testnet-1 the fee is written into the genesis, so it is the same on every node from block 1.

THE FEE COMES FROM THE VISIBLE BALANCE

Even shielded operations pay from the transparent side. Rule of thumb: keep at least 0.001 visible. If you don't, the wallet stops you before signing: “The network fee (0.000100) is paid from your TRANSPARENT balance — top it up first.”

MAX AND THE LOCAL CHECK

“max” fills balance – fee. The preview always shows “amount + fee”. If amount + fee exceeds your balance the Send button is disabled — the wallet refuses locally so a one-time key index is never spent on a transaction the chain would reject.

WHAT A REFUSAL LOOKS LIKE

“Chain refused: ... (nonce rolled back)”. The chain never takes money on a refusal (the fee is refunded inside the same block) and the wallet rewinds its key counter, so you simply try again with a smaller amount.

Where things live • troubleshooting

FILES (C:\Users\<you>\.hashkinetics\)

account.json
 seed, id, next_nonce — THE account
shield.json
 shielded master + one-time counters
disclosure-<id>.json
 packages you wrote for auditors

Back up account.json and shield.json together. Restoring account.json alone recovers the visible balance; shielded notes need shield.json too (deliberately — a one-time signing counter must never be guessed after a lossy restore).

SETTINGS

Prover: the field in the SHIELDED panel (default <https://prover.hashkinetics.org>). Change it only if you run your own hk-prove.
Network: fixed to the public RPC at rpc.hashkinetics.org.

IF SOMETHING LOOKS WRONG

- “Not on-chain yet” — tap Get test funds once; the faucet creates the account.
- “cooldown (retry in ~23h)” — one drip per IP per day. Ask a teammate to send you a little, or wait.
- Header says “connecting...” — no answer from rpc.hashkinetics.org; check your connection and press ↻ Refresh.
- The SHIELDED section closes by itself after an operation — click its header to reopen (known cosmetic issue, fix queued).
- Window too small to see the activity log with SHIELDED open — drag the window bigger; the layout stretches.
- “prover unreachable” — the public prover is down or blocked; try again in a minute or set your own hk-prove URL.
- “Chain refused ... nonce rolled back” — nothing was spent; read the reason, usually the fee. Adjust and retry.
- Accounts from staging-1 do not exist on testnet-1 — same seed, tap the faucet once, and you are re-created with a fresh balance.

What this wallet is — and is not

IS

Real: every click here produced a real consensus transaction on testnet-1 on 2026-09-02, with receipts (txids 194d4a0e..., 944362aa..., 5696eeba..., 22082712...). Every signature is hash-based; every shielded proof is a STARK verified in consensus.

IS NOT

Money. Test units have no value and nothing is for sale. The build is unsigned (SmartScreen warns). This is a testnet: the chain can be reset, and testnet-1 replaced staging-1 today — balances did not carry over.

NEVER

A master view key. Nobody — not the team, not a validator — can see your shielded notes. The only way in is a disclosure package you write, for one payment, on purpose.