

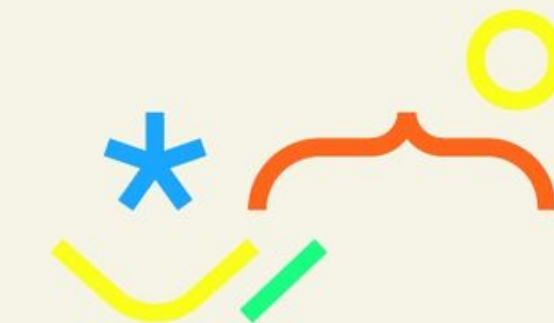


×



Commons

×



carbs

Delegate signing on the XRP Ledger without giving away the account.

Sessions the ledger enforces, opened from a post-quantum root on a Ledger Stax.

Protocol Innovation

Ledger · Protocol Innovation

NYC · 24–25 Oct 2026

SIGNING SESSION

Open session

Mode	C · XRP payments
Max spend	XRP 20, fees in
Max per payment	XRP 5
Valid for	10 minutes
Agent ID	A1E8-094F

Cannot change keys or signers

Inside the rules

tesSUCCESS

Outside, no fee

tefSESSION_LIMIT

On XRPL, a key holds all of an account's authority, or none.

APPS AND AGENTS

Too much power, or a prompt for every transaction.

A wallet, a game or an AI agent either holds your full key or asks you to approve each transaction. XLS-75 delegation gives rights to another funded account.

No expiry. No cap.

#657 delegate auto-expiry

#572 agent identity

EVERY ACCOUNT

A key that has signed stays exposed, for good.

Its public key sits on the ledger forever: a forgery target for a future quantum computer. Ripple's plan targets native post-quantum keys by 2028, without hardware wallets.

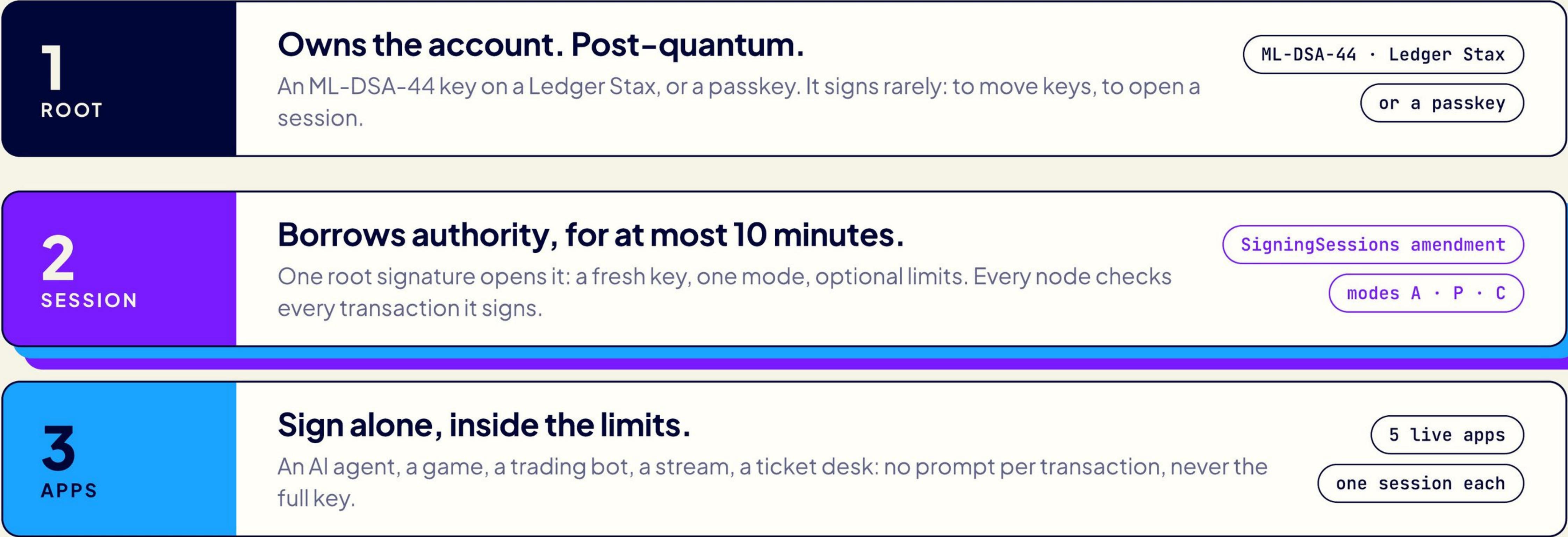
≈ 5.6 M accounts

76.8 B XRP behind exposed keys

Vet audit, Apr 2026

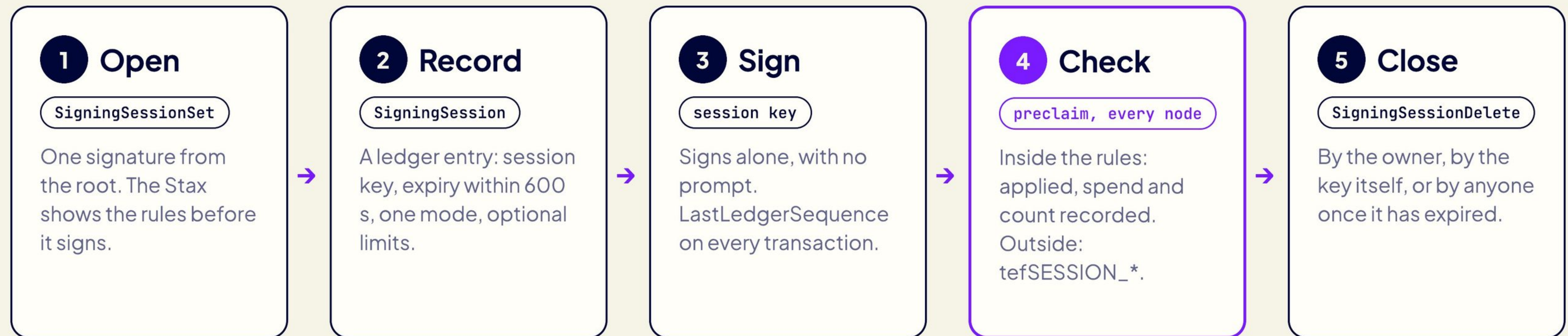
Split authority into three layers.

Each layer can do less than the one above it, for less time. Apps never touch the root.



The ledger enforces the limits, the Stax shows them, and a session key can never change who controls the account.

One signature opens a session. Every node enforces it.



✓ **Refusals never enter a ledger**

and never cost a fee: every session refusal is a tef code.

✓ **A session cannot change who controls the account**

No SetRegularKey, SignerListSet, PasskeyListSet or AccountSet.

✓ **An invariant checks every session transaction**

Keys, signers, passkeys and spend are re-checked after it applies.

Three modes. Each app gets the narrowest one.

A

All transactions

MAY SIGN

Every delegable transaction type, except the ones that touch account control.

BOUND BY

Time · a fee ceiling

FOR

An app you trust for ten minutes

P

Listed permissions

MAY SIGN

Only the 1 to 10 XLS-75 permissions the session names.

BOUND BY

Time · the list · a fee ceiling

FOR

A trading bot: OfferCreate, OfferCancel

C

Capped XRP

MAY SIGN

Direct XRP payments only.

BOUND BY

Time · a total cap, fees included · a fee ceiling

FOR

An AI agent with a budget

Optional, in any mode

Max per payment (C)

Max transaction count

Witness co-signer

Refusals

tefSESSION_TX_NOT_ALLOWED

tefSESSION_EXPIRED

tefSESSION_LIMIT

tefSESSION_NO_WITNESS

Batch where it helps. Never where it hides.

WHERE IT HELPS

✓ Open and pay with one approval

The session opens and the first payment goes out together, all or nothing.

Batch [SigningSessionSet, Payment]

✓ Revoke every session at once

One approval closes up to eight sessions per Batch.

Batch [SigningSessionDelete × 8]

✓ Rotate the key on every payment

Each payment also sets the next RegularKey, so it reveals only the key it retires.

Batch [Payment, SetRegularKey → next]

WHERE IT IS REFUSED

✗ A session key never signs a Batch

Inner transactions carry no signature of their own: a session could hide inside.

tesSESSION_TX_NOT_ALLOWED

✗ The Stax reads every inner transaction

It shows each one, and refuses a Batch it cannot read to the end.

0x6815

FOUND ON THE WAY

A key migration in one Batch returns tesSUCCESS and applies nothing. So the move to the post-quantum root is three transactions, with a proof in between.

The root: post-quantum, in a Ledger Stax.

MOVE AN ACCOUNT TO THE STAX IN THREE TRANSACTIONS

1

SetRegularKey → the Stax’s ML-DSA-44 key

Signed by the old master key.

2

A proof transaction, signed with ML-DSA-44

Shown in clear on the Stax before it signs.

3

asfDisableMaster

No classical key is left: the old key now gets **tefMASTER_DISABLED**.

Quantum exposure check

exposed

no-exposure-found

unknown

Any address: which of its keys is already on the ledger, and since which transaction. Mainnet is only read.

THE KEY

ML-DSA-44

FIPS 204 · module lattices · no known quantum attack

Public key	1,312 bytes
Signature	2,420 bytes
secp256k1, for scale	33 · ~72 bytes
Session keys	ML-DSA-44, fresh each time

Pure ML-DSA, not pre-hash: the Stax shows exactly the bytes it signs. The key comes from the 24 words (SLIP-21), so it returns after a reinstall.

Passkeys: the one-tap path, on both devices.

Separate from the XRP app. Both open the same sessions; only the XRP app on the Stax shows the rules.

Mac · Touch ID

classical, or PQ vault

KEY

A P-256 passkey, or an ML-DSA-44 key that Touch ID unlocks (WebAuthn PRF).

OPENS A SESSION WITH

One Touch ID.

ON THE LEDGER

The alphanet Passkey amendment, with our **fixPasskeyChallenge** and **fixP256StrictDer**.

SHOWS THE RULES?

No: the prompt shows the site's domain.

Ledger Stax · Security Key

post-quantum

KEY

An ML-DSA-44 passkey (COSE -48), made on the device.

OPENS A SESSION WITH

One press on the Stax (FIDO2 over USB).

ON THE LEDGER

PasskeyMLDSA, our amendment: each key bound to its PasskeyID.

SHOWS THE RULES?

No: FIDO shows the site. The rules are read in the XRP app.

First

An ML-DSA-44 passkey from a real Stax, accepted by an XRPL node: registration, payment, session (6.2 s and 4.2 s per signature).

Five apps, five sessions, one engine.

Each app gets the narrowest session that does its job. Beyond it, the ledger refuses.

C

MODE C

AI agent on a budget
Buys data from paid x402 APIs, on its own.

SESSION
cap 20 XRP
5 XRP per payment

REFUSED
The 500 XRP an injected prompt asks for

tefSESSION_LIMIT

C

MODE C

Hash Blaster
An arcade where every shot is a payment.

SESSION
cap 5 XRP
0.1 XRP per shot
300 shots

REFUSED
The auto-clicker past 300 shots

tefSESSION_LIMIT

P

MODE P

Grid trading
A bot quotes XRP/USD on the XRPL order book.

SESSION
OfferCreate
OfferCancel
200 tx

REFUSED
A Payment signed by the bot's key

tefSESSION_TX_NOT_ALLOWED

C

MODE C

Pay-as-you-go stream
Pays the provider every few seconds while it plays.

SESSION
cap 1 XRP
0.01 XRP per payment
600 tx

REFUSED
One payment above 0.01 XRP

tefSESSION_LIMIT

P

MODE P

Ticket desk
Mints event tickets as NFTs, alone.

SESSION
NFTTokenMint
50 tx

REFUSED
Sending XRP to an outside account

tefSESSION_TX_NOT_ALLOWED

Each opens with one approval; game, trading, streaming and minting also name a profile the Stax enforces. Live on the team's network.

Demo: open, act, get refused, expire.

- 1 Check a real account's quantum exposure**
mainnet, read only
- 2 The Stax signs the move to its ML-DSA-44 root**
clear-signed
- 3 Open a session: the rules appear on the Stax**
one signature
- 4 Five actions, no prompt**
session key alone
- 5 A stolen key tries to take over**
refused, no fee
- 6 The sixth payment hits the cap, then the session expires**
tefSESSION_LIMIT · tefSESSION_EXPIRED

```
$ pnpm --filter web live-run
[C] open                                tesSUCCESS
[C] payment 1..5                        tesSUCCESS
[C] payment 6                          tefSESSION_LIMIT
[A] set regular key                     tefSESSION_TX_NOT_ALLOWED
[A] burn fees                          tefSESSION_LIMIT
[A] other account                       tefBAD_AUTH
[expiry] after expiry                   tefSESSION_EXPIRED
[expiry] own close                      tesSUCCESS
fee charged on every refusal: false
```

Built and tested the way rippled is built.

TESTS

49 cases · 3,586 checks

SigningSessions suite: every case asserts its exact result code.

Mutation-proven

Break a rule on purpose, its test fails. Every rule.

1.32 M tests

Full rippled suite on the final tree: no failure from our code.

FOUND IN THE BASE, FIXED

fixPasskeyChallenge

Every WebAuthn signature refused where char is signed.

fixP256StrictDer

Anyone relaying a P-256 transaction could change its hash.

PasskeyMLDSA

Post-quantum passkeys, each key bound to its PasskeyID.

FIRSTS ON HARDWARE

ML-DSA-44 on a hardware wallet

3 payments signed by our Stax, validated on the public AlphaNet (24 Oct), one clear-signed.

A post-quantum passkey

From a real Stax, accepted by an XRPL node: registration, payment, session.

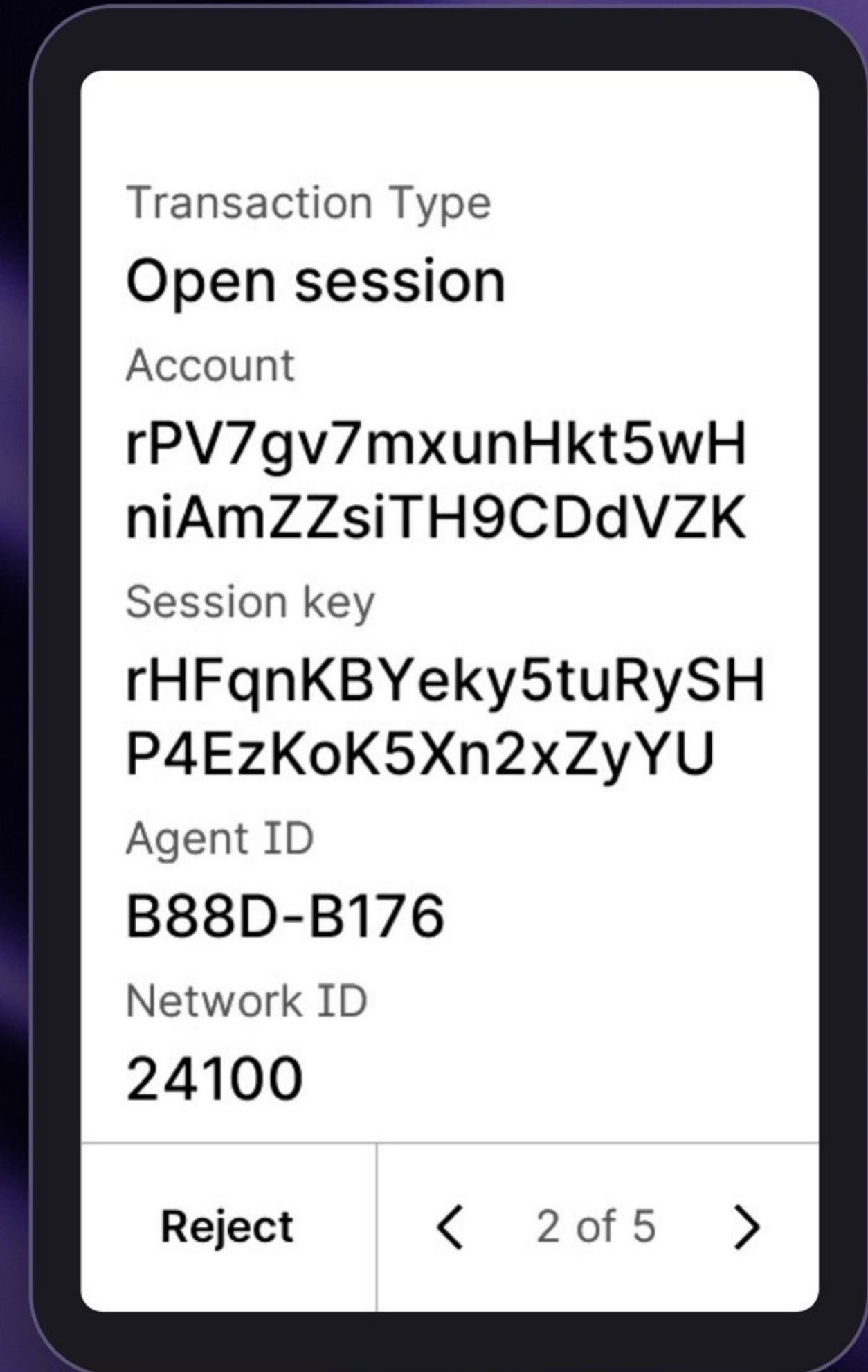
carbs

**A post-quantum root on the Stax,
and sessions it shows in clear.**

ML-DSA-44 signing for XRPL, clear-signed session rules, and an owner policy the device enforces.

Ledger · Protocol Innovation

XRPL Hackathon NYC · 24-25 Oct 2026



Our XRP app on Stax · emulator snapshot

Ledger and XRPL meet at the signature. That's where the gaps were.

“There is still no XRPL transaction Clear Signing.”

Ledger, XRPL NYC track brief

THE GAP

No hardware wallet signs XRPL with a post-quantum key.



Delegation is blind: a full key, or a prompt that shows a domain.



Nothing bounds what an app may ask the device.



WHAT CARBS ADDS

ML-DSA-44 in the XRP app, clear-signed, validated on the public AlphaNet.

Session rules shown in clear on the Stax, then enforced by the ledger.

An owner policy and per-app profiles, checked on the device before any review.

Three things the Stax now does for XRPL.

1

Signs with ML–DSA–44

A post-quantum key from the 24 words signs XRPL transactions, after the same clear review as a classical one.

APDU 0x10 · 0x11 · 0x12

2

Shows sessions in clear

Open session, Agent ID, Valid for, Max spend, Max per payment, Witness, Max transactions, and “Cannot change keys or signers”. A Batch is shown inner by inner.

never blind · 0x6815

3

Enforces the owner’s policy

Max spend, per payment, duration, allowed modes, witness, and five per-app profiles. Checked before any review.

above the policy · 0x6986

What the owner reads before a session exists.

Transaction Type

Open session

Account

rPV7gv7mxunHkt5wH
niAmZZsiTH9CDdVZK

Session key

rHFqnKBYeky5tuRySH
P4EzKoK5Xn2xZyYU

Agent ID

B88D-B176

Network ID

24100

Reject

< 2 of 5 >

Who

The account, the session key and its Agent ID, which the agent prints too.

Valid for

5 minutes

Fee

XRP 0.000012

Max spend

XRP 40

Max per payment

XRP 10

Witness

rawnHFk1gPQeEBC88
cXbetXLqw3hnpk4pE

Reject

< 3 of 5 >

How much, how long

The limits the ledger will enforce: duration, max spend, max per payment, witness.

Allows

XRP payments only, fees included

Note

Cannot change keys or signers

Reject

< 4 of 5 >

What it can never do

XRP payments only, fees included. It cannot change keys or signers.

The human approves on the Stax. Software signs inside. The rest is refused.

THE HUMAN APPROVES, ON THE STAX

Moving the account to the ML-DSA-44 root

three transactions, each reviewed

Opening a session

its rules on screen, one approval

Anything above the session

a bigger purchase goes back to the owner

SOFTWARE SIGNS, ALONE

The session key, for 10 minutes at most

agent, game, trading, streaming, minting

No prompt per transaction

inside the limits the owner read

Never the root key

it stays on the device

REFUSED, WHATEVER SOFTWARE SAYS

A session it cannot show in full

on the Stax · 0x6815

Above the owner's policy

on the Stax · 0x6986

Anything outside the session

on the ledger · tefSESSION_*

ML-DSA-44 on a Stax: 36 KB of RAM, no shortcuts.

1,312 B

public key

2,420 B

signature

2,048 B

max signed message

36 KB

SRAM on the Stax

DESIGN DECISIONS

- ◆ **Pure ML-DSA over the fully buffered message**

Pre-hash would sign a digest the screen cannot show. The Stax displays exactly the bytes it signs.

- ◆ **Buffers overlay the transaction context**

About 31 KB of statics before the overlay, 25 KB after, in the low-RAM variant of the SDK.

- ◆ **A SHA-256 lock on the review**

While a review is on screen, an approval signs only the bytes that were shown.

- ◆ **Key derived by SLIP-21 from the 24 words**

The same key comes back after a reinstall: verified on our Stax.

Signed on our Stax, accepted by XRPL nodes.

XRP APP · PUBLIC ALPHANET · 24 OCT

Three payments signed with ML-DSA-44 by our Stax, validated **tesSUCCESS.**

The first is clear-signed: the app parsed it and showed type, amount and destination. Key 1,312 B, signature 2,420 B, verified with @noble/post-quantum first.

TRANSACTION

46F4D08446F73FDF4DA648EB5E050B7B
F0C8FA882B35B53B8D90E2BFD6F6F3EE

ACCOUNT

rGcT27HiGhoJWYRxqg9jcnPboGD4RGuLLm

SECURITY KEY APP · A SEPARATE PATH

The Stax as a post-quantum passkey.

Ledger's FIDO2 app, extended with ML-DSA-44 credentials (COSE -48). Our PasskeyMLDSA amendment verifies them, each key bound to its PasskeyID.

- ✓ **Registration: a 1,312-byte ML-DSA-44 key**
- ✓ **A payment signed by the passkey: **tesSUCCESS****
- ✓ **A session opened by the passkey: **tesSUCCESS****

6.2 s and 4.2 s per signature, approval included. FIDO2 over USB, not the DMK. Still untested: the Chrome ceremony.

A library beats a one-off: we extended Ledger's own kit.

device-signer-kit-xrp, extended

getPqPublicKey, signTransactionPq and getSessionPolicy, in the kit's own style. Its 106 upstream tests run unedited next to ours.

Device Management Kit only

WebHID, no legacy ledgerjs package anywhere in the client.

A written device contract

Every APDU, status word and screen line in docs/device-contract.md. The client predicts the review line for line.

Tested like an app

cmocka unit tests, 700 Ragger snapshots on five devices, 448 M fuzz mutations under ASan and UBSan, no crash.

61 entries written as we built. Five would have saved the most.

- 1 ML–DSA is not in the Stax’s OS crypto library**
It is not in cx.export: an app compiles the SDK sources itself, on a tight RAM budget.
- 2 Clear–signing a new XRPL type touches about eight places**
A missed one silently falls back to blind signing, or shows “Unknown”.
- 3 Who adds the STX\0 prefix is unstated**
The app adds it; the DMK forwards bytes unchanged. A client that adds it signs the wrong bytes.
- 4 Loading from macOS has no documented route**
Docker cannot pass USB. A locked device answers 0x5515, an open app 0x6D00.
- 5 Deterministic ML–DSA keygen is in an internal header**
No documented path to keys recoverable from the 24 words.

61

entries

548

minutes lost, measured

5

time-savers on top

Every app, agent and wallet on XRPL needs bounded authority.

WHO NEEDS IT

AI agents

About a quarter of ledger activity, paying with x402.

Games, trading, streaming

Many small signatures, no prompt each time.

Wallets

Passkeys and hardware, one approval per session.

WHAT IT UNLOCKS

Delegation that expires and caps

Enforced by every node, not by an app's promise.

A way out of key exposure

A guided move for the 5.6 M exposed accounts.

Hardware-grade approval

The Stax approves the rules once, not every transaction.

NEXT

Upstream

Offer the XLS draft and the four amendments.

Ledger

Send the signer-kit extension as a pull request.

Harden

Coverage-guided fuzzing, the Chrome passkey ceremony.

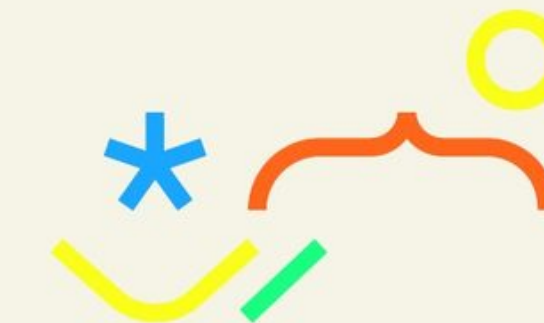


×



Commons

×



carbs

Delegate signing without giving away the account.

TRY IT

LIVE APP

carbs-kappa.vercel.app

CODE

github.com/STOOOKEEE/carbs

SPEC

[docs/XLS-Sessions.md](#)