

Private zUSD on the public ZSA testnet — NozyWallet evidence

NozyWallet / LEONINE-DAO · Campaign 2026-09-16 · Attachment for forum.zcashcommunity.com · Suggested thread: ZSA Testnet (topic 56884)

Network: <https://zsa.methyl.cc> · Faucet: <https://faucet.zsa.methyl.cc> · HRP: uregtest1

This note reports a full private-asset loop on the dedicated OrchardZSA / ZSA developer network (**not** Zcash mainnet, **not** Ironwood): fund with faucet tZEC → scan → issue a custom asset named **zUSD** → transfer → burn. It is evidence for wallet and protocol discussion. Testnet zUSD is a named custom asset for ZIP 226/227 exercise — **not** a redeemable dollar.

What we proved

Step	Result
Reach public ZSA LWD without mixing Ironwood mainnet deps	Yes — isolated nozy-zsa toolkit with QEDIT OrchardZSA pins
Receive / decrypt faucet tZEC	Yes — OrchardZSA compact ciphertext is 84 bytes
Issue custom asset zUSD (ZIP 227)	Yes — mined
Transfer zUSD privately (ZIP 226)	Yes — mined
Burn part of zUSD supply (ZIP 226)	Yes — mined

Evidence log

#	Action	Result	Txid / detail
1	Derive uregtest1 address	From Nozy seed (coin type 133)	Funded via faucet.zsa.methyl.cc
2	Scan / balance	Unspent tZEC notes visible	Compact ciphertext 84B
3	Issue 100 zUSD	Mined @ height 171970	205248d77373a81ee3e9b7fd7b328d87504dc16aaf0f682a3abf75885fae7821
4	Inspect issue	value=100 + 0-value reference note	ZIP 227 first issuance shape
5	Transfer 10 zUSD (acct0→acct1)	Mined	396b21e477cf983dca9225f53dc7096a880590bd54bdb46d4517382e7136ae06
6	Burn 5 zUSD	Mined (~height 172002)	827c3c670bc0da643728b49bed4b229e5d3d87c17a483295c9d9dc2327a362e6

After burn (approx): account 0 ≈ 85 zUSD · account 1 ≈ 10 zUSD.

Asset identity (issuer ZIP-32 issuance key + name zUSD):

asset_desc_hash: 1113d0c924e01ad4eff0bd58e92eeb70ac7e1ebfac571756f6e3b4aeba23ad20

AssetBase: 774b66fdae3b49737f9d9f8c7194c08d3401ef981b771ccb6a88a6c8b4912f11

Loop we ran

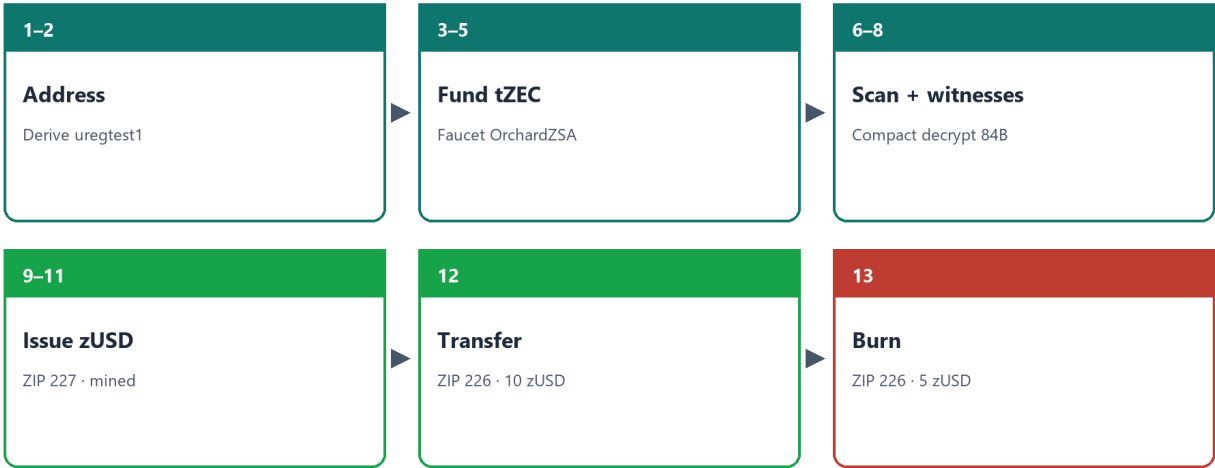
- 1 Load wallet seed → derive uregtest1 Orchard address (account 0).
- 2 Request faucet tZEC to that address.
- 3 Compact-scan via <https://zsa.methyl.cc> and trial-decrypt notes.
- 4 Build Merkle witnesses (fetch full txs for issuance commitments when needed).
- 5 ZIP 227 issue of zUSD; fee paid in native shielded tZEC (ZIP-317).
- 6 ZIP 226 transfer of zUSD to a second account under the same seed.
- 7 ZIP 226 burn of part of the supply.

Diagrams are on the next pages at full size for readability.

Figure 1 — Sprint loop (proven)

Sprint 1 loop on ZSA testnet

Private custom-asset path: address → fund → scan → issue zUSD → transfer → burn

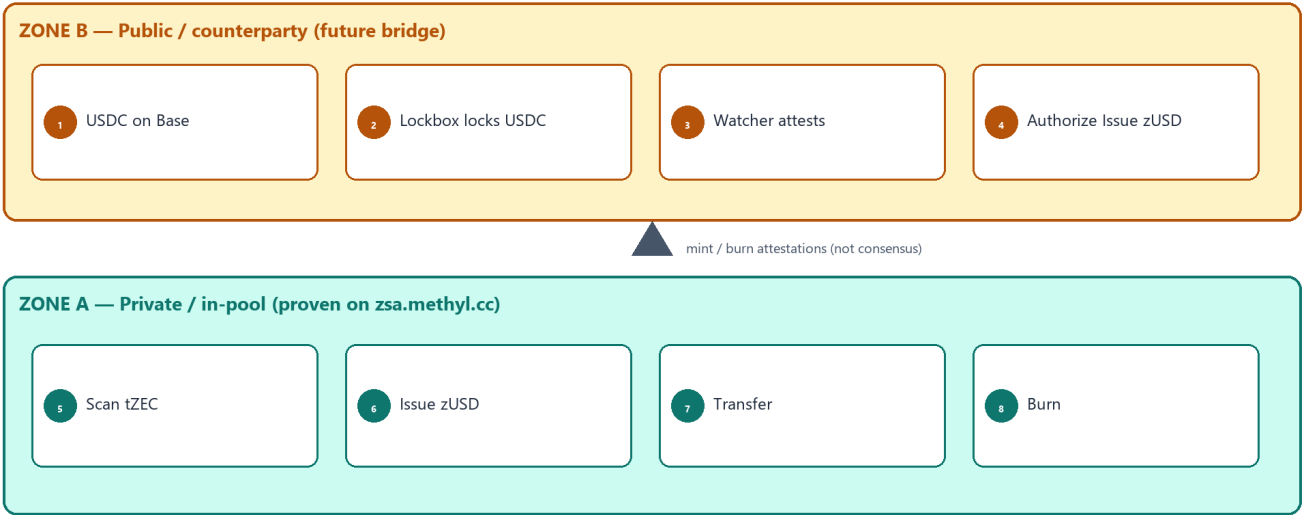


Evidence: issue 205248d7... @ 171970 · transfer 396b21e4... · burn 827c3c67...

Address → fund → scan → issue zUSD → transfer → burn

Figure 2 — Private in-pool vs future public wrap

Architecture: Zone B (public) ↔ Zone A (private)



Zone A proven on testnet; Zone B USDC wrap is future design only

Figure 3 — Proven sequence (steps 1–13)

Sequence 1–13 — proven on ZSA testnet (zUSD issue / transfer / burn)

Proven Zone A	Issue / transfer	Burn
1	Load wallet seed (ZIP-32 coin type 133) User → Nozy	DONE
2	Derive uregtest1 Orchard address (account 0) Nozy	DONE
3	Request tZEC from faucet User → Faucet	DONE
4	Shielded faucet send (OrchardZSA) Faucet → Zebra	DONE
5	Compact blocks published (84-byte ciphertext) Zebra → LWD	DONE
6	GetBlockRange + trial-decrypt (balance) Nozy → LWD	DONE
7	Return unspent tZEC notes + cmx stream LWD → Nozy	DONE
8	Build witnesses (BridgeTree + full txs) Nozy	DONE
9	ZIP 227 Issue zUSD (isk + fee spend) Nozy	DONE
10	SendTransaction V6 + zip-233 Nozy → LWD	DONE
11	Mempool → mine issue tx @ 171970 LWD → Zebra	DONE
12	ZIP 226 Transfer 10 zUSD (acct0 → acct1) Nozy → LWD	DONE
13	ZIP 226 Burn 5 zUSD (destroy supply) Nozy → LWD	DONE

What we actually ran: fund, issue, transfer, burn

Figure 4 — Future wrap sequence (steps 14–18)

Sequence 14–18 — future public wrap (not proven on this net)

Future Zone B bridge

14	Deposit / lock USDC on Base User → Lockbox	NEXT
15	Lock event attested by watcher Lockbox → Watcher	NEXT
16	Authorize 1:1 Issue zUSD to user UA Watcher → Nozy	NEXT
17	User burns zUSD to redeem User → Nozy → LWD	NEXT
18	Attest burn → release USDC Watcher → Lockbox	NEXT

Not proven on this net — product / bridge target only

On this testnet we only exercised the private in-pool path. A future USDC lock ↔ private mint path is bridge / issuer design and was **not** proven here.

Operator notes that bit us

- 1 **Compact scan alone misses issuance commitments** — GetTransaction is required or spends hit an unknown Orchard anchor.
- 2 **V6 parsing needs zip-233** or lightwalletd can mis-parse amounts.
- 3 **Public net enforces ZIP-317** — zero-fee issue is rejected; pay fees in tZEC.
- 4 **First issuance** includes a 0-value reference note plus the valued note (ZIP 227).
- 5 **Isolate OrchardZSA QEDIT pins** from Ironwood orchard 0.15 used for mainnet ZEC.

What this is not

- Not mainnet ZSA / NU schedule news.
- Not a claim that Nozy desktop/extension already ships a ZSA UI.
- Not a live USDC lockbox or attestation service.
- Not a third-party audit — this is our wallet-side loop against the public testnet.

Status

Piece	Status
Public ZSA LWD + faucet	Used successfully
Issue / transfer / burn zUSD	Done — txids above
Main Nozy desktop / extension wiring	Next
USDC lock ↔ private mint bridge	Design only

Links

- ZSA Testnet forum: <https://forum.zcashcommunity.com/t/zsa-testnet/56884>
- Public LWD: <https://zsa.methyl.cc>
- Faucet: <https://faucet.zsa.methyl.cc>
- NozyWallet: <https://github.com/LEONINE-DAO/Nozy-wallet>

Happy to compare notes with other wallet / tooling teams on OrchardZSA edges (issuance witnesses, V6/zip-233, ZIP-317 fees).

— *NozyWallet / LEONINE-DAO*