FALCON MULTI-CHAIN WALLET & BRIDGE

Testnet Implementation Report

Network ID 1001 · Date: 28 July 2026 · Repository: Falcon-faucet-wallet

Policy: Bridge-only mint — no free bootstrap of F-USDC, FETH, FBNB, or FBTC.
Custody model: Custodial lock-mint (EVM) and native BTC custody + claim-mint; off-chain deposit relays; not fully trustless.

This report describes the complete multi-wallet and multi-chain bridge system as deployed on testnet: product model, key domains, all four live bridge routes, architecture, verified mint transactions, wallet RPC design, ops services, code map, security, and remaining work.

1. Product Model

1.1 Three wallet tabs

- Falcon — Native FALCON + bridged IOUs (F-USDC, FETH, FBNB, FBTC). Falcon-512 passkey vault.
- Multi-chain — Native deposit wallets for ETH (Sepolia), BTC (testnet P2PKH), BNB (BSC testnet). Same passkey encrypts EVM + BTC keys.
- Bridge — Lock-mint In (and F-USDC Out). Uses Multi-chain EVM and BTC keys.

1.2 One passkey, three key domains

- Falcon (r…) — Ledger payments, trust lines, F-asset send, bridge-out memos
- EVM (0x…) — Sepolia ETH/USDC, BSC testnet BNB, FETH/FBNB locks. ETH and BNB share the same 0x key.
- BTC — Testnet m…/n… P2PKH (mainnet 1… also derived). Native BTC receive/send and BTC → FBTC bridge.

Same address on Sepolia, BSC testnet, and BSC mainnet. Balances are per network. Sending mainnet BNB to the 0x on BSC mainnet does not credit BSC testnet.

1.3 Backup JSON (v3)

File type: `qxrp-falcon-wallet-backup`, version 3. Encrypted payload includes falcon_secret, address/publicKey/label, evm_private_key/evm_address, btc_private_key/btc_address/btc_address_mainnet. Re-export builds a new snapshot of the browser vault. Restore accepts versions 1–3.

2. Live Bridge Routes (Testnet)

All bridge-ins: collateral verified on source chain → deposit relay mints 1:1 IOU on Falcon. No free mint of QUC / ETH / BNB / BTC currency except via verified source-chain deposits.

Route	Status	Source	Falcon currency	Relay
USDC → F-USDC	Live (In+Out)	Sepolia USDC	QUC	qxrp-bridge-relay
ETH → FETH	Live (In)	Sepolia WETH	ETH	qxrp-feth-relay
BNB → FBNB	Live (In)	BSC testnet WBNB	BNB	qxrp-fbnb-relay
BTC → FBTC	Live (In)	Bitcoin testnet	BTC	qxrp-fbtc-relay + claims

Coordinator service status (2026-07-28): all five units active.

2.1 Token / lock / custody addresses

Sepolia (chain id 11155111)

- USDC (Circle test): 0x1c7D4B196Cb0C7B01d743Fbc6116a902379C7238
- WETH: 0xfFf9976782d46CC05630D1f6eBAb18b2324d6B14
- USDC lock: 0x2dae31Cbf2E3a418d617081985661fCD0117b75C
- WETH/FETH lock: 0x11808B5Cda14d4144dbD2279f92f447e0f8F8F1d
- Lock owner (ops EOA): 0x64BA18002B6E72fE443f3F8a146cE529250Db107

BSC testnet (chain id 97)

- WBNB: 0xae13d989daC2f0dEbFf460aC112a837C89BAa7cd
- WBNB/FBNB lock: 0x682D60Bbf8dE13065C71cbF35c1dAdAa23E79938
- Lock owner: same 0x64BA…Db107

Bitcoin testnet3

- FBTC custody (P2PKH): mxuamPnEtoMaiRnBnAUnrCZeXTYPVX4hik
- Custody mainnet (reserved): 1JPdULhG5mvKwKJa4bWR2HMKfTwgbReTqE

Falcon (network 1001) issuers

- F-USDC / QUC → rPh77fAAmvbVuMQQP9H9JKtyTFuhRjp3Fk

- FETH / ETH → rNn8xd3hbeTEAcEmRQae8xVaKshAj7HrED
- FBNB / BNB → rf8NZLdcwxrXAnPpptTeenQcAJW75uj7E
- FBTC / BTC → rnvzCKcBU7G8Kb9JXHwEKTHiK9aTrZAqWT

3. Architecture

3.1 EVM lock-mint (USDC, ETH/WETH, BNB/WBNB)

Browser wallet (passkey vault) → FalconCollateralLock on Sepolia or BSC → DepositCreated event → bridge-deposit-relay.py → Falcon Payment IOU (F-USDC / FETH / FBNB).

3.2 Native BTC claim-mint (FBTC)

Multi-chain BTC wallet sends P2PKH to custody mxuamPnE… → Wallet POST claim → bridge-btc-deposit-relay.py verifies explorer tx → mints currency BTC. Wallet UX: one Bridge action (passkey unlock → send BTC to custody → register claim → mint FBTC). No WBTC shown or required.

3.3–3.7 Supporting components

- Contract: qXRP/contracts/FalconCollateralLock.sol — deploy via qXRP/scripts/deploy-falcon-lock.js
- User path: approve + deposit(amount, falconAccount) → DepositCreated event
- EVM deposit relay: scripts/bridge-deposit-relay.py
- BTC deposit relay: scripts/bridge-btc-deposit-relay.py + fbtc-claims-server.py (:8099)
- Withdraw relay: F-USDC only today (bridge-withdraw-relay.py + sepolia-withdraw memo)
- Wallet same-origin proxies (CSP-safe): /api/wallet/btc-balance, btc-proxy, bnb-balance, bnb-rpc, /api/bridge/btc

4. End-to-End Flows

- USDC → F-USDC: TrustSet QUC → approve → lock.deposit → mint. Bridge Out via memo sepolia-withdraw.
- ETH → FETH: TrustSet ETH → wrap WETH → approve → feth_lock.deposit → mint. No Bridge Out yet.
- BNB → FBNB: TrustSet BNB → wrap WBNB → approve → fbnb_lock.deposit → mint (via bnb-rpc proxy). No Bridge Out yet.
- BTC → FBTC: TrustSet BTC → one passkey action sends to custody + claim → mint. No WBTC. No Bridge Out yet.

5. Verified Bridge Mint Ledger (2026-07-28)

FETH — 2 mints

1) 13:13:36Z | 0.00005 ETH | r44mzkf… | Sepolia 0x840c79f8… | Falcon D01327A5…

2) 15:44:23Z | 0.1 ETH | rKqqPLM… | Sepolia 0xb4c54c25… | Falcon 468692B3…

FBNB — 1 mint

1) 15:50:38Z | 0.15 BNB | rKqqPLM… | BSC 0xcf7fe6e6… | Falcon 10E550D8…

FBTC — 1 mint

1) 16:25:01Z | 0.001 BTC (100000 sats) | rKqqPLM… | BTC 9cb1fede… | Falcon B4A2FC35…

F-USDC — 47 mints total (sample recent)

- 09:23:09Z | 30 USDC | rMpmiVGj… | sepolia 0xd6a7eb74… | falcon 10107FAF…
- 17:17:28Z | 5 USDC | rMpmiVGj… | sepolia 0x55bca076… | falcon 49E097FE…
- Full history held in /var/lib/qxrp-bridge/relay_state.json

6. Ops (Coordinator 46.224.0.140)

Services: systemctl status qxrp-bridge-relay / qxrp-feth-relay / qxrp-fbnb-relay / qxrp-fbtc-relay / qxrp-fbtc-claims

State paths: /var/lib/qxrp-bridge/{usdc,feth,fbnb,fbtc}-bridge.json, *_relay_state.json, fbtc_claims.json, btc-custody.json, /var/lib/qxrp-stables/stables_state.json

Live mint counts: F-USDC 47 · FETH 2 · FBNB 1 · FBTC 1

7. Remaining Work

- FETH / FBNB / FBTC Bridge Out (parameterize withdraw / release)
- Mainnet locks + multi-sig REQUIRED ≥ 2
- Mainnet BTC custody policy + confirmation depth
- Proof-of-reserves / multi-party mint
- Bech32 / Taproot BTC addresses (today P2PKH only)
- DEX liquidity for FETH / FBNB / FBTC
- Company entity / custody policy before public mainnet bridge

8. Security

- Relays hold issuer Falcon secrets on the coordinator. Compromise unauthorized mint of that IOU.

- EVM locks hold ERC-20; testnet often 1-of-1 multi-sig.
- BTC custody is ops-controlled P2PKH; FBTC mint depends on explorer attestation + claim registration.
- Browser never sends private keys to the API; only signed blobs / raw txs / claim metadata.
- Bridge is custodial attestation, not a light-client bridge.

9. Quick Reference — User Flows

- Testnet BTC: Multi-chain → BTC → Receive → P2PKH faucet
- tBNB: Multi-chain → BNB → Receive → BSC testnet faucet
- Sepolia ETH/USDC: Multi-chain → ETH → Receive / faucets
- Mint F-USDC: Bridge → USDC → F-USDC (trust line first)
- Mint FETH: Bridge → ETH → FETH (wrap + trust line)
- Mint FBNB: Bridge → BNB → FBNB (wrap + trust line)
- Mint FBTC: Bridge → BTC → FBTC (one action; no WBTC)
- Full backup: Export falcon-backup v3 after all keys exist

10. Summary

The Falcon multi-chain wallet is a single passkey vault covering Falcon, shared EVM (ETH+BNB), and BTC. Four bridge-in routes are live on testnet with verified mints:

Asset	Mints	Bridge Out
F-USDC	47	Yes
FETH	2	Not yet
FBNB	1	Not yet
FBTC	1 (native BTC custody)	Not yet

Full document on disk: qXRP-faucet-wallet/docs/MULTI-CHAIN-IMPLEMENTATION.md
Ops companion: qXRP/docs/ops/MULTI_CHAIN_BRIDGE.md

Compiled from deployed testnet state on coordinator 46.224.0.140 and wallet/qXRP source, 28 July 2026.