lokblok

SALES INFORMATION SHEET

Lokblok Personal Hot Wallet Demonstrator

Hardware-Rooted MPC | Online Signing | Zero Persistent Keys

2-of-3
Threshold Signature Scheme default quorum

0
Persistent key shares — ever

Hot
Connected, hardware-secured

Overview

The Lokblok Personal Hot Wallet Demonstrator shows how digital assets can be managed using hardware-rooted threshold cryptography and zero-trust execution environments — while remaining fully connected to the internet for a fast, convenient signing experience.

Reference Implementation

This is not a consumer wallet product. It is a working demonstrator showing how Lokblok's hardware architecture and SDK can power and accelerate time to market for a personal MPC hot wallet — one that gives consumers a level of security that exceeds even what's available to institutions today.

Not in software | **Not in memory** | **Not in the cloud**

All signing calculations are executed inside the Toughkey HSM — nowhere else.

Use Case — Who Is This For?

The Personal Hot Wallet is designed for high-net-worth individuals and active participants in digital asset markets who need institutional-grade security without sacrificing the speed and convenience of an online wallet. Lokblok enables hardware-anchored security without ever storing keys in software, memory, or the cloud.

- High-Net-Worth Individuals
- Family Offices
- Professional Investors
- Crypto-Native Entrepreneurs
- Institutions & Custody Providers

The Problem with Traditional Wallets

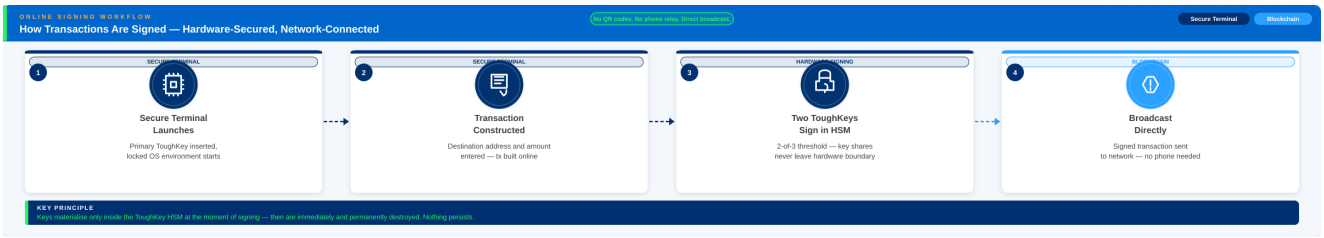
Traditional wallets (hardware or software) all share the same flaw: keys or key fragments exist somewhere. If attackers find the right device, interface, or backup, the assets can be stolen.

Approach	Risk
Single hardware wallet	One private key stored on one device — total loss if compromised
Multisig wallets	Multiple full private keys must each be protected separately
Software MPC	Key shares stored in cloud servers or application memory

With Phantom Secrets, keys never persist outside certified hardware — not even in fragments.

How the Lokblok Hot Wallet Works

The hot wallet demonstrator uses Phantom Secrets MPC in Toughkey for Threshold Signature Scheme generation. No persistent key shares are ever stored, and all signing calculations are executed inside the Toughkey HSM. The wallet connects directly to the network while maintaining the same hardware-rooted security as the cold wallet.



On the surface it looks and feels like any quorum-based signing. The difference is what Phantom Secrets does beneath it.

Step-by-Step Detail

1

Secure Terminal Launches

Primary Toughkey inserted. Locked-down, isolated, hardware-rooted signing environment starts. Unlike the cold wallet, network connectivity is permitted.

2

Transaction Constructed

User enters destination address and amount. System constructs the unsigned transaction. Connects directly to the blockchain — no QR code, no phone relay needed.

3

Two Toughkeys Sign

First Toughkey (already inserted) part-signs the transaction. Second Toughkey is inserted and password entered. Signing completes entirely inside the HSMs.

4

Broadcast to Blockchain

The signed transaction is broadcast directly to the network by the Secure Terminal. No phone or intermediary device needed.

But Phantom Secrets is Different

- **Traditional hardware wallets** store a full private key in one device
- **Multisig** stores multiple full private keys across devices
- **Software MPC** stores key shares in cloud servers or application memory

With Phantom Secrets there are no stored keys or key shares at all. The key is only calculated and exists at the point of use inside hardware, and burned immediately afterwards.

Key Features

Hardware-Rooted MPC Signing

Threshold signatures executed entirely inside certified Toughkey HSMs.

Hot Wallet Convenience

Connects directly to the blockchain, but is as secure as typical cold wallet storage

Multi-Device Threshold Approval

Two physical Toughkeys must be present to authorise any transaction. No single device can act alone.

Secure Terminal Environment

Locked-down signing environment resistant to malware and OS compromise. Hardware-rooted and purpose-built.

Configurable Quorum Models

Default 2-of-3 threshold. Any quorum level can be configured, 3-of-5, 4-of-7, or beyond.

Phantom Secrets Architecture

No stored keys or key shares. Keys materialise only at the point of use inside hardware and are burned immediately.

WHY IT'S BETTER

Five advantages over traditional hardware wallets and software wallets

lokblok.co

No exposed private keys

Keys never appear in system memory or software.

Reduced attack surface

Compromising software or servers cannot steal funds.

Hardware-rooted security

Transactions require physical Toughkey hardware present.

Safer than seed phrases

No reliance on fragile paper backups or mnemonics.

Future-ready architecture

Built on Phantom Secrets - the most advanced MPC architecture available.

What This Demonstrator Proves

The Lokblok Personal Hot Wallet Demonstrator shows that hot storage security and transaction workflows, can be as secure as cold wallet storage. Hardware-based MPC dramatically reduces attack surface, and institutions can deliver consumer wallets with institutional-grade protection. It is a foundation for next-generation personal custody solutions.

Online Convenience + Hardware Security

Fast, direct signing without sacrificing the protection of hardware-rooted MPC.

Software Compromise is Not Enough

No software path to key material - hardware and physical presence required.

Designed for Those Who Cannot Afford Compromise

Security anchored in hardware for individuals managing significant digital wealth.

"Security anchored in hardware. Designed for those who cannot afford compromise."

lokblok

Ready to see the Hot Wallet in action?

Contact us to arrange a live demonstration.

lokblok.co | info@lokblok.co

© 2026 Lokblok Inc. | Commercial in Confidence