lokblok

SALES INFORMATION SHEET

Lokblok Personal Cold Wallet Demonstrator

Hardware-Rooted MPC | Air-Gapped Signing | Zero-Trust Execution

2-of-3
Threshold Signature Scheme Default signing quorum

Only
works when there's no network connection

Air
gapped by design

Overview

The Lokblok Personal Cold Wallet Demonstrator shows how digital assets can be secured using hardware-rooted threshold cryptography, air-gapped threshold signature scheme signing, and zero-trust execution environments.

> **Reference Implementation**
> This is not a retail wallet product. It is a reference implementation demonstrating how Lokblok's hardware architecture and SDK can enable financial institutions, security vendors, or device manufacturers to build the next generation of personal cold wallets. The demonstrator proves that institutional-grade digital asset security can be delivered to individuals without exposing private keys to software, networks, or cloud infrastructure.

Use Case | Who Is This For?

The Personal Cold Wallet architecture is designed for users who hold significant digital assets and cannot rely on traditional consumer wallets that expose keys to software or require fragile backup mechanisms such as seed phrases. Lokblok enables a vault-like security model where transactions can be performed while the wallet itself never connects to the internet.

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

The Problem with Traditional Hardware Wallets

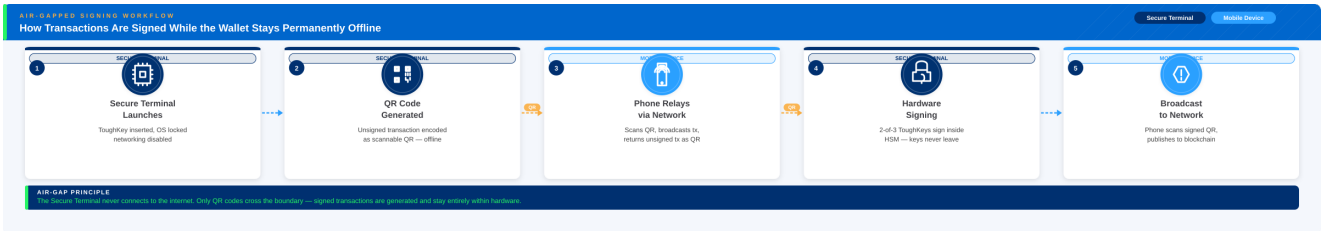
Most existing wallet solutions store keys or fragments somewhere. If attackers compromise the right device, interface, or backup, the assets can be stolen.

Approach	Risk
Single hardware wallet	One private key stored in one device, total loss if compromised
Multisig wallets	Multiple private keys must each be protected separately
Software MPC	Key shares stored in software or cloud infrastructure
Seed phrases	Easily lost, copied, or stolen, no recovery without the phrase

Lokblok: Keys never persist outside certified hardware, not even in fragments.

How the Lokblok Cold Wallet Works

The cold wallet demonstrator uses hardware-based Phantom Secrets MPC and Threshold Signature Schemes running entirely inside hardware security modules. The wallet never connects to the internet, a phone acts purely as a QR code relay between the offline Secure Terminal and the blockchain network.



Step-by-Step Detail

1

Secure Terminal Launches

The primary Toughkey is inserted and a Secure Terminal session begins. The OS locks down, networking is disabled, and a dedicated signing environment is created. If networking is detected, the Secure Terminal and wallet refuses to operate.

2

Transaction Created (Offline)

The user enters a destination address and amount. The system generates a QR code containing an unsigned transaction. Nothing has been signed yet — the wallet remains completely offline.

3

Phone Acts as Network Relay

A phone scans the QR code, connects to the blockchain, builds the transaction, and returns an unsigned transaction as a new QR code. The phone cannot sign — it is a network messenger only.

4

Hardware-Based Signing

The transaction returns to the Secure Terminal. Two physical Toughkeys sign using a 2-of-3 threshold model. Signing runs entirely inside HSMs — key shares never leave hardware, never appear in memory, never reconstructed in software.

5

Transaction Broadcast

The signed QR code is scanned by the phone and broadcast to the blockchain. The Secure Terminal never touched the internet throughout the entire process.

Key Features

Hardware-Rooted MPC Signing

Threshold signatures executed entirely inside certified hardware security modules. Key shares never leave hardware.

Air-Gapped Transaction Workflow

Transactions executed while the wallet remains fully offline. QR codes are the only data crossing the air-gap boundary.

Multi-Device Approval

Multiple Toughkeys must be physically present to authorise any transaction. No single device can act alone.

Secure Terminal Environment

Locked-down signing environment resistant to malware and OS compromise. Networking is hardware-enforced off.

Flexible Quorum Models

Configurable threshold policies such as 2-of-3 or 3-of-5. Any quorum model can be deployed to match governance needs.

Designed for Phantom Secrets

We eliminate persistent key shares entirely — no key material stored anywhere, at rest or in transit.

WHY IT'S BETTER

Five advantages over traditional hardware wallets and software custody solutions

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 hardware modules present.

Safer than seed phrases

No reliance on fragile paper backups or mnemonics.

Future-ready architecture

Evolves into Phantom Secrets — zero at-rest key material.

What This Demonstrator Proves

The Lokblok Personal Cold Wallet Demonstrator shows that cold storage security can coexist with usable transaction workflows, 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.

Cold Storage + Usable Workflows

Transactions can be executed securely without the wallet ever going online.

Hardware MPC Reduces Attack Surface

No software path to key material — hardware boundaries enforce security.

Institutional Security for Individuals

Vault-grade protection delivered in a personal custody format.

"Institutional-grade digital asset security, delivered to individuals - without exposing private keys to software, networks, or cloud infrastructure."

lokblok

Ready to see the Cold Wallet in action?

Contact us to arrange a live demonstration of air-gapped signing.

lokblok.co | info@lokblok.co