QUILLON VAULT

A Post-Quantum Hardware Wallet with Physical Air-Gap Security

Q-NarwhalKnight Project

`https://quillon.xyz`

Version 1.0 — February 2026

"As thin as a credit card. As secure as a vault. As elegant as jewelry."

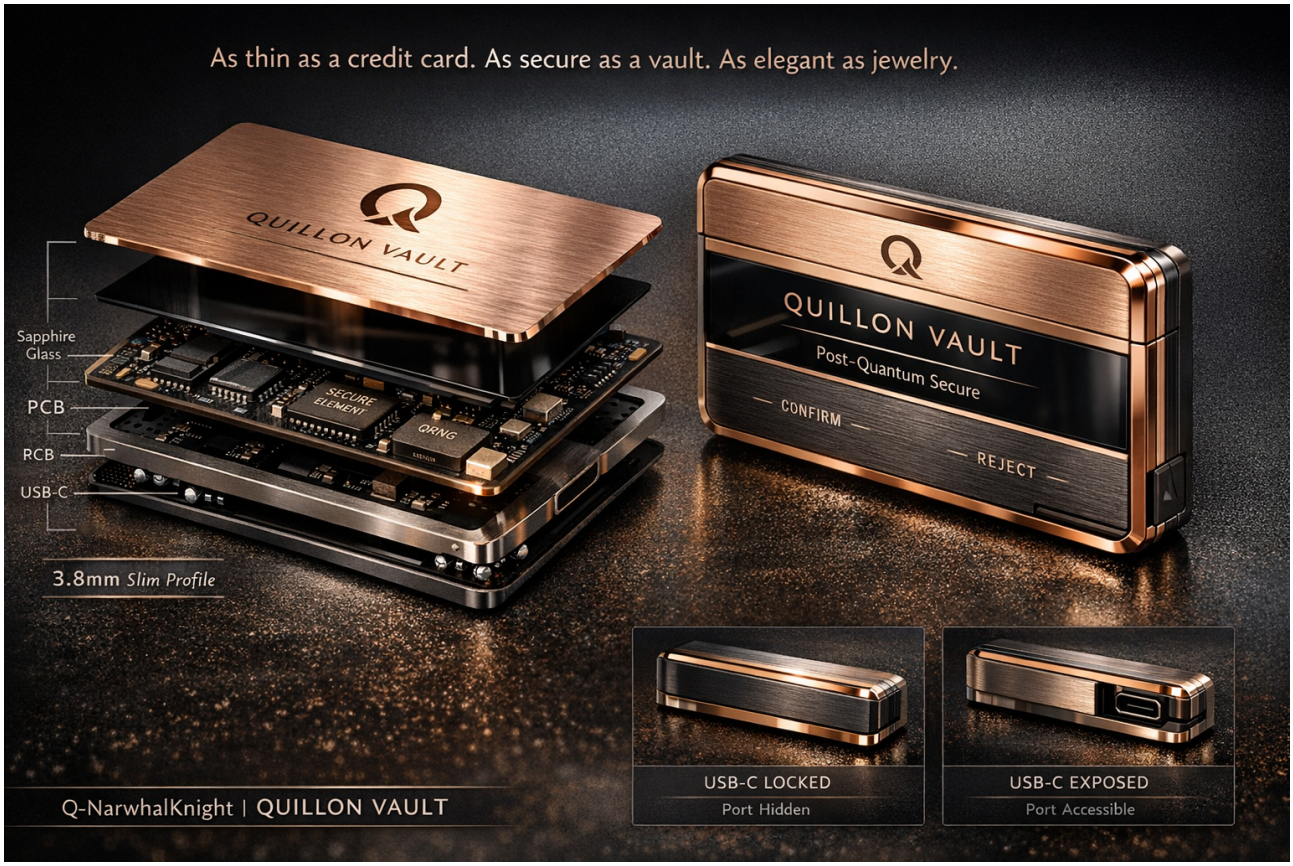

Figure 1: QUILLON VAULT — exploded component view (left), assembled device with OLED display and confirm/reject buttons (right), and USB-C slide mechanism in locked and exposed states (bottom insets).

Abstract. We present **QUILLON VAULT**, a credit-card-form-factor hardware wallet designed for the Q-NarwhalKnight post-quantum blockchain. At 85.6 mm × 54 mm × 3.8 mm and 28 g, it is among the thinnest hardware signing devices ever proposed. The defining innovation is a *machined titanium sliding frame* that physically disconnects the USB-C data lines when locked — creating a true hardware air gap that no software exploit can bridge. Internally, a dedicated Quantum Random Number Generator (QRNG) chip provides information-theoretically unpredictable entropy for key

generation, while NIST FIPS 204 Dilithium5 (ML-DSA, Level 5) signatures execute entirely within a tamper-resistant secure element. Every transaction is dual-signed with both Ed25519 and Dilithium5, providing security against both classical and quantum adversaries. The USB channel is encrypted via Kyber-1024 (ML-KEM) key encapsulation combined with AES-256-GCM. This paper details the mechanical design, security architecture, cryptographic protocols, and manufacturing considerations for the QUILLON VAULT.

1. Introduction

The security of cryptocurrency hardware wallets rests on a simple principle: *private keys must never leave the device*. Yet existing wallets remain vulnerable along two axes that current designs inadequately address.

First, the USB interface is a permanent attack surface. When a hardware wallet is plugged in, the host computer can enumerate it, probe its descriptors, and — in the presence of firmware vulnerabilities — extract secrets or inject malicious payloads. Every minute a wallet remains connected is a minute of exposure.

Second, all production hardware wallets today generate their keys using deterministic pseudo-random number generators (PRNGs) seeded by classical entropy sources. These are computationally secure under current assumptions, but offer no information-theoretic guarantees. A sufficiently powerful adversary — including a future cryptanalytically relevant quantum computer (CRQC) — could potentially reconstruct the PRNG state.

The QUILLON VAULT addresses both problems with two hardware-level innovations:

1. A **physical air-gap mechanism**: a precision-machined titanium frame that slides along ceramic ball-bearing rails, actuating a hardware switch that electrically disconnects the USB-C D+/D− data lines. When the frame is in the LOCKED position, the wallet is electrically unreachable — not merely software-isolated, but circuit-broken.
2. A **Quantum Random Number Generator** (QRNG) chip that derives entropy from quantum shot noise, providing keys whose randomness is guaranteed by the laws of quantum mechanics rather than computational hardness assumptions.

These are complemented by a fully post-quantum cryptographic stack: Dilithium5 signatures, Kyber-1024 encrypted USB communication, and SHA-3-256 hashing.

2. Design Philosophy

The QUILLON VAULT was designed under three constraints:

Thinness. The device must fit in a standard card slot. We target the ISO/IEC 7810 ID-1 footprint (85.6 mm × 54 mm) at a thickness of 3.8 mm — thinner than two stacked credit cards.

Security by physics. Every critical security property must have a physical enforcement mechanism, not merely a software one. Air gaps should be air gaps. Randomness should be quantum.

Elegance. A security device that users find beautiful will be carried; one they find ugly will be left in a drawer. The titanium frame, sapphire glass, and precision slide mechanism are not cosmetic additions — they are adoption enablers.

3. Mechanical Architecture

3.1 Form Factor

The device dimensions are summarized in Table 1. The thickness budget is tightly constrained:

Layer	Thickness
Titanium top shell (Gr. 5)	0.6 mm
Sapphire glass OLED window	0.3 mm
PCB + components (4-layer)	2.0 mm
Titanium bottom shell	0.6 mm
Magnetic slide rail	0.3 mm
Total	**3.8 mm**

Table 1: Physical specifications.

Parameter	Value
Length	85.6 mm
Width	54 mm
Thickness	3.8 mm
Weight (Ti)	28 g
Weight (Al)	22 g
Shell	Grade 5 titanium
Display	Sapphire crystal
PCB	4-layer, 0.8 mm

3.2 The Slide Mechanism

The central mechanical innovation is the sliding titanium frame. An 8 mm linear translation exposes the USB-C port. The mechanism consists of:

- **Precision slide rails** machined into both top and bottom shells, with ceramic ball bearings (Si_3N_4) for zero-wobble linear travel.
- **N52 neodymium magnet detents** at both the LOCKED and UNLOCKED positions, providing a satisfying tactile "click" and holding the frame securely in either state.
- **A hardware disconnect switch**: a spring-loaded contact embedded in the slide rail that is physically depressed only when the frame reaches the UNLOCKED position. This switch completes the USB-C D+/D− circuit. In the LOCKED position, the circuit is *broken* — an air gap enforced by mechanics, not software.

The electrical implication is critical: when the frame is closed, the USB-C data lines are physically interrupted. No amount of software exploitation on the host computer can establish communication with the wallet. The power lines (VBUS/GND) are also disconnected, preventing even side-channel power analysis via the USB connector.

3.3 Exterior Finish

All edges feature a 45° chamfer with mirror polish, contrasting against the brushed face. Six material variants are planned:

1. **Obsidian** — PVD black titanium, gold logo
2. **Titanium** — Natural Grade 5, silver logo
3. **Rose** — Rose gold PVD, white logo
4. **Stealth** — Matte black ceramic, no logo
5. **Arctic** — White zirconia ceramic, Ti frame
6. **Carbon** — Carbon fiber inlay, Ti frame

4. Electronic Architecture

4.1 Component Selection

Table 2 lists the key electronic components. Every part was selected for the intersection of security properties, physical size, and power characteristics compatible with a bus-powered, battery-less design.

Table 2: Key electronic components.

Part	Specification
SE	ATECC608B (2×3 mm)
MCU	STM32L4S5, Cortex-M4, 120 MHz, TrustZone
Display	SSD1306 0.42" OLED, 72×40 px
USB	USB-C mid-mount (8.9×2.5 mm)
QRNG	IDQ Quantis (3×3 mm)
Flash	W25Q16JV, 2 MB SPI NOR
Haptics	LRA ×2 (4×4×1.5 mm)
Buttons	Capacitive touch (flush)

4.2 Secure Element: ATECC608B

The ATECC608B is a dedicated cryptographic coprocessor with hardware-protected key storage (keys never leave the die), side-channel resistance (DPA, SPA, fault injection), a monotonic counter for replay attack prevention, secure boot attestation, and a hardware TRNG (supplemented by the external QRNG).

Private keys are generated *inside* the secure element using entropy from the QRNG chip and are used for signing without ever being exposed to the MCU, the host computer, or firmware update processes.

4.3 Quantum Random Number Generator

The IDQ Quantis QRNG chip generates random bits from quantum vacuum fluctuations (shot noise on a photodetector). Unlike PRNGs, the output is *information-theoretically random* — its unpredictability is guaranteed by quantum mechanics, not computational hardness. This provides:

- Key generation entropy that cannot be predicted even by a quantum computer

- Nonce generation that eliminates the risk of nonce reuse via PRNG state compromise
- Seed material for the BIP-39 mnemonic that is physically unpredictable

4.4 MCU: STM32L4S5 with TrustZone

The STM32L4S5 provides ARM TrustZone hardware isolation, partitioning the processor into a **Secure world** (cryptographic operations, SE communication, signature construction) and a **Non-secure world** (USB protocol, display rendering, user interaction).

A compromised non-secure world cannot access secure-world memory, registers, or peripherals. Additional protections include stack canaries, ASLR, and a hardware watchdog timer for fault injection resistance.

4.5 Display and User Interaction

The 0.42" SSD1306 OLED display, protected by a 0.3 mm sapphire crystal window, shows transaction details (recipient, amount, token), wallet addresses, firmware version, and PIN entry prompts.

Two flush-mount capacitive touch buttons (CONFIRM and REJECT) with LRA haptic feedback provide physical transaction authorization. The haptic pattern differs between confirm (single pulse) and reject (double pulse) for accessibility.

5. Security Architecture

The QUILLON VAULT implements defense-in-depth across five layers.

5.1 Layer 1: Physical Security

- **Titanium enclosure**: Grade 5 Ti-6Al-4V provides drill and cut resistance
- **Epoxy-potted PCB**: Optically opaque, thermally resistant encapsulation prevents physical probe access
- **Tamper mesh**: Fine copper mesh on the PCB detects intrusion and triggers key wipe
- **Holographic seal**: Tamper-evident seal over the shell seam

5.2 Layer 2: Secure Element Isolation

The ATECC608B enforces that key material never crosses the die boundary, all signing operations execute within the SE, side-channel countermeasures operate at the silicon level, and a monotonic counter prevents replay.

5.3 Layer 3: Firmware Integrity

Secure boot chain requires firmware signed by Quillon's release key (stored in SE). TrustZone memory isolation prevents cross-world leakage. Stack canaries and ASLR harden against memory corruption. A hardware watchdog detects voltage glitching and clock manipulation.

5.4 Layer 4: Post-Quantum Cryptography

Transaction signatures: Dual-signature mode. Every transaction is signed with both Ed25519 (classical, 64-byte) and Dilithium5 / ML-DSA (post-quantum, NIST Level 5, 4,627-byte). If a CRQC breaks Ed25519, Dilithium5 remains valid. If lattice cryptanalysis advances, Ed25519 remains secure. Both must verify.

Key generation: QRNG-derived entropy, processed through SHA-3-256, provides seed material for both key pairs. QRNG output is XORed with the SE's internal TRNG as a defense-in-depth entropy source.

USB encryption: Host-to-wallet communication uses **Kyber-1024** (ML-KEM, FIPS 203) for key encapsulation, establishing a shared secret for **AES-256-GCM** authenticated encryption. Even a compromised USB stack cannot extract signing keys.

Hashing: SHA-3-256 (FIPS 202) for all internal hashing. SHA-3-256 provides ∼128-bit security against Grover's quantum search.

5.5 Layer 5: User Verification

The OLED displays *exact* transaction details — what the user sees is what the SE signs. A physical button press is required; remote signing is impossible. PIN policy: 3 wrong attempts triggers a 24-hour lockout; 10 wrong attempts triggers permanent key wipe. Recovery via BIP-39 mnemonic on titanium seed card.

6. The Physical Air Gap

The slide mechanism's security properties deserve emphasis. In the **LOCKED** state:

$$\text{USB D+/D}^- \longrightarrow \underbrace{[\ \text{GAP}\ ]}_{\text{switch open}} \longrightarrow \text{MCU} \qquad (1)$$

The spring-loaded contact in the slide rail is mechanically retracted, creating a physical break in the D+ and D− traces. No electrical signal can traverse this gap. The VBUS power line is similarly disconnected, preventing USB enumeration, firmware exploitation, side-channel power analysis, and EM emanation analysis via the USB cable as antenna.

In the **UNLOCKED** state (frame slid 8 mm), the spring contact is depressed, completing the circuit:

$$\text{USB D+/D}^- \xrightarrow{\text{contact}} \text{MCU} \qquad (2)$$

This is, to our knowledge, the first hardware wallet where the USB data connection has a *user-controlled physical disconnect* as an integral part of the device form factor — not an afterthought (USB cap) or an accessory (Faraday bag), but a machined precision mechanism built into the device's primary interaction paradigm.

7. Cryptographic Protocol

7.1 Key Generation

1. QRNG chip generates 512 bits of quantum-random entropy
2. SE internal TRNG generates 512 bits of classical entropy
3. Both sources are XORed, then processed through SHA-3-512
4. Output seeds both Ed25519 and Dilithium5 key pairs
5. BIP-39 mnemonic derived from the combined 512-bit seed
6. Key pairs generated *inside the SE*, never exported

7.2 Transaction Signing

1. Host sends transaction over Kyber-1024 encrypted channel
2. MCU renders transaction details on OLED display
3. User taps CONFIRM or REJECT
4. If confirmed: MCU passes transaction hash to SE
5. SE signs with Ed25519, then with Dilithium5
6. Both signatures returned over encrypted channel
7. SE increments monotonic counter (prevents replay)

7.3 Firmware Updates

New firmware images must be signed with Quillon's Dilithium5 release key. The SE verifies the signature before allowing flash writes. The OLED displays the version change for user confirmation, and a physical button press is required to authorize. The previous firmware is retained in a backup partition for rollback, and the update process is atomic (power-loss-safe).

8. Threat Model

The following threats are addressed:

Malware on host. USB exploitation, firmware injection. *Mitigated by:* Physical air gap; Kyber-1024 encrypted channel; signed firmware updates.

Physical theft. Device stolen, keys extracted. *Mitigated by:* PIN lockout; titanium shell; epoxy-potted PCB; tamper mesh triggers key wipe.

Side-channel. Power analysis, EM emanation, timing. *Mitigated by:* SE with DPA/SPA resistance; air gap disconnects power; constant-time crypto.

Supply chain. Tampered device before delivery. *Mitigated by:* Holographic seal; secure boot attestation; device certificate chain.

Quantum adversary. Shor's algorithm on ECDSA/EdDSA. *Mitigated by:* Dual-sign Dilithium5 + Ed25519; QRNG keys; Kyber-1024 USB encryption.

PRNG weakness. Predictable key generation. *Mitigated by:* QRNG chip (quantum shot noise);

XOR with SE TRNG; information-theoretic randomness.

Evil maid. Device tampered while unattended. *Mitigated by:* Tamper mesh; holographic seal; secure boot detects firmware modification.

9. Comparison with Existing Wallets

Table 3: Feature comparison.

Feature	Status vs. Competitors
Thickness	**3.8 mm** (vs. 8–15 mm)
Physical air gap	**USB slide disconnect** (unique)
PQ signatures	**Dilithium5 Level 5** (none offer PQ)
QRNG	**IDQ Quantis** (none offer QRNG)
Dual-sign	**Ed25519 + Dilithium5** (unique)
Encrypted USB	**Kyber-1024 + AES-256** (unique)
Secure Element	ATECC608B (comparable)
Shell material	**Grade 5 Titanium** (vs. plastic)

No existing production hardware wallet offers post-quantum signatures, quantum random number generation, or a physical USB disconnect mechanism. The QUILLON VAULT is, to our knowledge, the first design to combine all three in a credit-card form factor.

10. User Experience Flow

The interaction model prioritizes simplicity:

1. **Slide frame open** — magnetic click at UNLOCKED
2. **Insert USB-C** — OLED wakes, shows wallet address
3. **Authorize transaction** — OLED shows amount, recipient, token; user taps CONFIRM or REJECT
4. **Unplug USB-C** — OLED enters sleep
5. **Slide frame closed** — magnetic click at LOCKED; USB-C electrically disconnected and physically concealed

The entire signing interaction takes approximately 5 seconds. The device requires no battery — it is entirely bus-powered via USB.

11. Manufacturing and Cost

Table 4: Bill of materials (10K volume).

Component	Cost
Titanium shells (CNC + PVD)	$18.00
PCB + assembly (4-layer)	$8.00
ATECC608B Secure Element	$1.20
STM32L4S5 MCU	$6.00
0.42” OLED + sapphire	$4.00
USB-C mid-mount connector	$0.80
IDQ Quantis QRNG	$12.00
Slide mechanism	$5.00
LRA haptic motors (×2)	$1.50
Flash + passives + assembly	$3.00
Total BOM	**$59.50**
Retail (Titanium)	$149.00
Retail (Ceramic)	$199.00

The titanium shells are 5-axis CNC machined with PVD coating. The slide mechanism uses injection-molded rail channels with press-fit ceramic ball bearings and N52 neodymium magnets epoxied into machined pockets.

12. Packaging

The QUILLON VAULT ships in a magnetic-close presentation box with soft-touch matte finish and foil-stamped Q logo:

- Device in molded microfiber tray
- Braided USB-C cable (30 cm)
- **Titanium recovery seed card** — fireproof, waterproof, for metal-stamping the 24-word BIP-39 mnemonic
- Quick-start guide with QR code

The titanium seed card ensures the backup survives conditions that would destroy paper or plastic.

13. Integration with Q-NarwhalKnight

The QUILLON VAULT is the native hardware signing device for the Q-NarwhalKnight post-quantum blockchain [1]. The integration is natural because Q-NarwhalKnight already requires dual Ed25519 + Dilithium5 signatures, SHA-3-256 transaction hashing, and Kyber-1024 for P2P encryption.

Supported operations include native QUG transfers, QUGUSD stablecoin transactions, custom token (QRC-20) transfers, DEX swap authorization, smart contract interaction, and RWA token management.

14. Future Work

- **Bluetooth Low Energy**: Wireless signing with Kyber-1024 encrypted channel
- **NFC tap-to-sign**: Contactless transaction authorization at point-of-sale
- **Multi-signature**: m-of-n threshold signing across multiple devices
- **Biometric auth**: Fingerprint sensor with SE-backed template storage
- **SQIsign migration**: When isogeny-based signatures mature, the crypto-agile firmware allows switching from Dilithium5 to SQIsign for 204-byte PQ signatures

15. Conclusion

The QUILLON VAULT demonstrates that post-quantum hardware security, physical air-gap isolation, and elegant industrial design are not mutually exclusive. By building the security architecture around physical enforcement mechanisms — a machined titanium slide that breaks USB circuits, a QRNG chip that derives entropy from quantum mechanics, and a secure element that performs Dilithium5 signing without ever exposing key material — we achieve security properties independent of software correctness assumptions.

The device fits in a card slot at 3.8 mm, weighs 28 g, and requires no battery. It is the first hardware wallet designed from the ground up for the post-quantum era, and the first where the USB connection has a user-controlled physical disconnect built into the device's primary form factor.

The QUILLON VAULT is designed for Q-NarwhalKnight. Visit `https://quillon.xyz`.

References

[1] Q-NarwhalKnight Project, "Q-NarwhalKnight: A Post-Quantum DAG Consensus System," Technical whitepaper, 2026.

[2] NIST, "FIPS 204: Module-Lattice-Based Digital Signature Standard (ML-DSA)," 2024.

[3] NIST, "FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)," 2024.

[4] NIST, "FIPS 202: SHA-3 Standard," 2015.

[5] L. Ducas et al., "CRYSTALS-Dilithium: A Lattice-Based Digital Signature Scheme," TCHES, 2018.

[6] R. Avanzi et al., "CRYSTALS-Kyber: A CCA-Secure Module-Lattice-Based KEM," IEEE Euro S&P, 2018.

[7] D.J. Bernstein et al., "High-Speed High-Security Signatures," J. Cryptographic Engineering, 2012.

[8] Microchip Technology, "ATECC608B CryptoAuthentication Device Datasheet," 2020.

[9] ID Quantique, "Quantis QRNG Chip: True Random Number Generation," 2023.

[10] M. Palatinus and P. Rusnak, "BIP-39: Mnemonic Code for Generating Deterministic Keys," 2013.