mineracks

Self-hosted bitcoin infrastructure · Brisbane

DISTRIBUTED · POLICY-ENFORCED · MULTISIG HSM

Your treasury refills itself. By your rules, on your keys.

An exchange keeps a few percent of funds hot. The rest sits in cold storage — until it moves to top the hot wallet back up. That refill is the largest, least-automated transaction your business makes, and today it runs on one of two shaky foundations: a manual signing ceremony, or a custodian who holds your keys.

The hot wallet is the small target.

You already rate-limit it, monitor it, and accept it can be drained. The catastrophic loss is the cold reserve behind it — and the only time it's reachable is the moment it opens to refill the hot side.

Every refill is a ceremony or a custodian.

Either people hand-sign with hardware wallets under time pressure when the hot wallet runs dry, or a SaaS custodian signs for you. One is slow and error-prone; the other isn't your keys.

> *An attacker doesn't need your hot wallet. They need the moment your cold wallet opens to fill it — and they need that moment to be governed by software they can reach, not hardware you hold.*

THE GAP THE MULTISIG HSM CLOSES

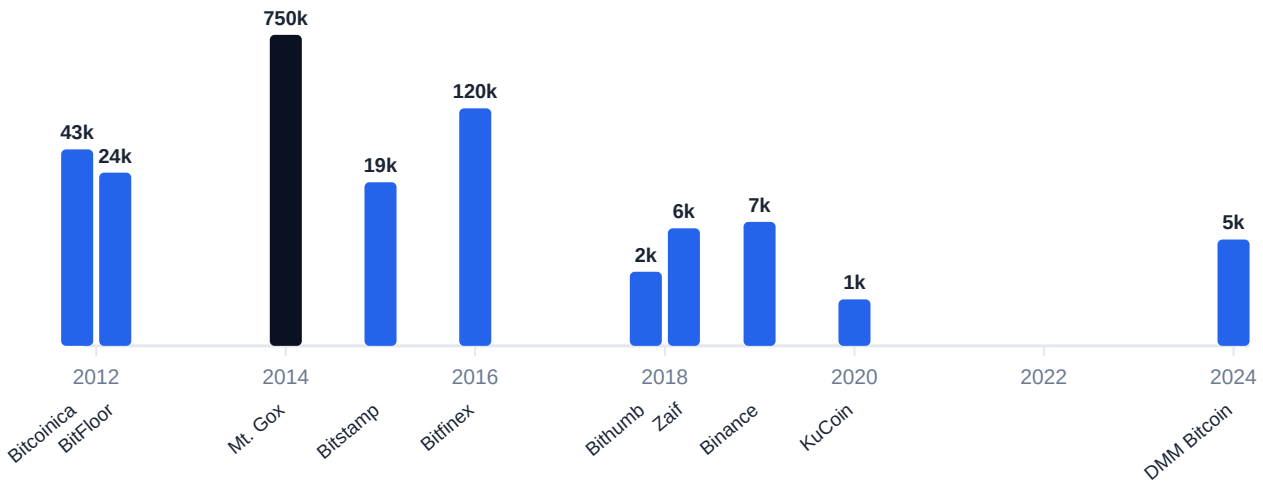
Real hardware. A Coldcard in HSM mode, signing on a host in the rack — one of three independent signers.

A hacked server drains a hot wallet almost every year.

Putting a signing key on an internet-connected server is the bet exchanges keep losing — it is the single most common way custodial Bitcoin is stolen. Since 2012, there has been a hot-wallet/server drain in nearly every year.

BITCOIN LOST PER INCIDENT

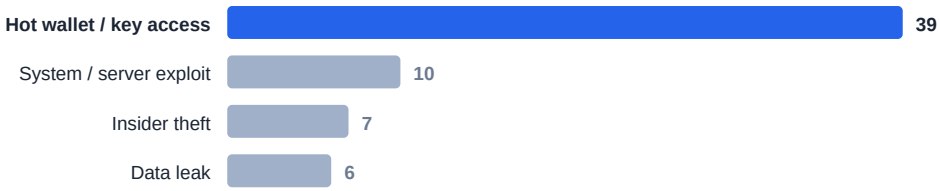
log scale · BTC at each hot-wallet/server breach



A loss in nearly every year — on the order of **~1,000,000 BTC** in total, concentrated in Mt. Gox (~750k) and Bitfinex (~120k). Mixed-asset hacks show the Bitcoin portion; values priced at the time, disputed figures given as ranges. **Sources →**

MOST COMMON EXCHANGE ATTACK VECTOR

incidents, 2009–2024 (n=62 categorised, CEX)



Source: Bello et al., Frontiers in Blockchain (2025), 220-incident dataset — centralised-exchange classes.

1 · So: an HSM

Keep the signing key on tamper-resistant hardware it can **never leave**. A fully-owned server still can't extract it — the most-exploited failure mode is gone.

2 · One isn't enough

A single device on a single host is still a single point: own that one box, or coerce that one operator, and it signs. The bottleneck moved, it didn't vanish.

3 · So: a multisig HSM

2-of-3 across **independent hosts**, each enforcing its own policy. No single hacked server *or* insider moves funds — and any one signer can fail without freezing the rest.

THE REFILL PROBLEM

Two bad options, every single refill.

The cold→hot refill is where sovereignty, automation and policy collide — and today you get to pick two at most. Here's what's actually on the table.

OPTION A · DO IT YOURSELF

Manual cold multisig.

Secure keys — but a human ritual.

- ✕ People, hardware wallets, a room and a checklist — often at 3am when the hot wallet drains
- ✕ Can't run unattended; doesn't scale with volume or staff turnover
- ✕ Every signer sees and approves by hand — slow, and irreversible if they get it wrong
- ✕ Key-holders become the bottleneck *and* the insider-risk surface

You hold the keys. You also hold the pager.

OPTION B · HAND IT OFF

Custodial / MPC platform.

Automated and fast — but not your keys.

- ✕ The platform's software holds (a share of) the signing keys — you're trusting their stack
- ✕ Their SOC2, their insurance, their breach response — their compromise becomes yours
- ✕ Basis-points on reserves, forever; pricing built for institutions, not sovereignty
- ✕ Policy lives in a vendor console you don't control and can't fully audit

Fast and hands-off — by giving up custody of the bulk of your funds.

“

*Nobody ships all three at once: **automation**, **hardware keys you physically hold**, and **policy that can't be overridden in software**. That's the whole reason this exists.*

WHAT'S MISSING FROM BOTH OPTIONS

THE MINERACKS APPROACH

A cold tier that signs its own refills — by policy, no human.

Three independent hardware signers — Coldcards in HSM mode — each on a separate host, ideally a separate site. A keyless coordinator builds the refill transaction and fans it to any two. They check it against their own on-device rules and auto-sign. The signed refill broadcasts to your hot wallet. No human in the loop — and no single machine can move a satoshi.

Every refill gated on the hardware

A per-transaction cap, a velocity limit (max per hour/day), and an address whitelist that allows *only* your own hot-wallet deposit addresses. Break a rule and the secure element refuses to sign — no software path around it.

No single point of compromise — or failure

2-of-3 across separate hosts and sites. Own one signer and you move nothing. Lose one signer to a reboot, outage or dead device and refills carry on. Lose two and funds simply freeze — safe.

Keys you hold · a coordinator that holds none

The automation layer carries no keys, so its compromise can't move funds. The rules and the signing live on the Coldcards' secure elements. The coordinator only proposes; the hardware decides.

Need a bigger, one-off move? A human-gated surge.

Everyday refills run untouched — no human involved. When you deliberately want a larger spend, the owner enters a one-time code from a normal authenticator app, and **only then** will 2-of-3 sign above the everyday cap — still bounded by a separate **on-device surge ceiling** the coordinator can't exceed. The coordinator merely relays your code; the secret never leaves the Coldcards and your phone. Automation for the routine, a deliberate human gate for the exceptional.

AN AUTOMATED REFILL, START TO FINISH

STEP 1 Trigger

Hot wallet low

Balance falls below your floor — automatically detected

STEP 2 Propose

Keyless build

Coordinator drafts the refill PSBT from a watch-only wallet

STEP 3 Sign

Any 2 of 3

Two Coldcards check policy & auto-sign — no human

STEP 4 Refill

Broadcast

Signed top-up lands in your hot wallet on-chain

Don't take our word for it — a working 2-of-3 runs on real Bitcoin signet at ***multisighsm.com****. Every policy decision and transaction is inspectable on a public explorer.*

SECURITY MODEL · FOR THE REVIEWER WHO ASKS "WHAT IF IT'S BREACHED?"

Assume the server is owned. Now what?

Every serious custody review reduces to one question: what happens when a server is compromised, an operator goes rogue, or a data centre dies? Here's the honest answer, failure by failure.

COORDINATOR FULLY COMPROMISED

Can't steal — bounded by hardware.

- Holds **no keys** — can't sign or forge; every spend still needs two Coldcards
- Can't send **off your whitelist** — at worst it refills *your own* hot wallet early
- Can't exceed the devices' **velocity ceilings** — the hard catastrophic bound

Worst case is a capped, premature refill of your own addresses — not a theft.

SIGNER HOST(S) COMPROMISED

One moves nothing; two must beat the silicon.

- Own **one** host → zero: it needs two, and the key never leaves the secure element
- Own **two** → still capped by each device's on-device cap + velocity + whitelist
- An attacker must defeat **two independent secure elements**, not two Linux boxes

The host is a courier; the policy and the key live on the chip.

A HOST — OR A WHOLE SITE — LOST

Lose one, keep running; lose two, freeze safe.

- 2-of-3 across **independent failure domains**, ideally one offsite
- Any one signer down (outage, reboot, dead device) → refills continue
- Two down → funds **freeze, never stolen** — and resume when one returns

No single outage stops you; no single breach moves funds.

NO SINGLE POINT TO ATTACK OR LOSE

The limit is derived from the chain.

- The global velocity cap is computed **from the blockchain**, not one server's file
- Any coordinator replica recomputes it — nothing to corrupt, nothing to lose
- Replicas run across the same independent sites as the keys

There's no one box whose failure or tampering changes the answer.

The math is bounded — on purpose.

We show our working: a fully-compromised coordinator can move at most **1.5× a single signer's per-period velocity ceiling** (two signatures burned per unit of value). Set each ceiling to **two-thirds of your chosen limit** and the worst case equals that limit — enforced on hardware, not software.

HOW IT COMPARES

Where it fits — and where it doesn't.

Honest positioning beats a feature grid. Here's how the distributed policy HSM lines up against the options exchanges actually use to guard reserves and refill the hot side.

APPROACH	KEYS YOU PHYSICALLY HOLD	RUNS UNATTENDED	POLICY ON THE HARDWARE	NO VENDOR TO TRUST	COST
Single hot-wallet signer *one server signs everything*	~	✓	✗	✓	low
Manual cold multisig *humans sign with hardware wallets*	✓	✗	~	✓	low $
MPC custody SaaS *Fireblocks, BitGo, Copper…*	✗	✓	~	✗	high $$$
Enterprise HSM / vault *Ledger Enterprise, Thales, CloudHSM*	✓	~	✓	~	high $$$
Collaborative custody *Unchained, Casa, Nunchuk*	✓	✗	~	~	mid $$
mineracks distributed policy HSM *2-of-3 Coldcards · self-hosted*	✓	✓	✓	✓	low $

✓ yes ✗ no ~ partial / depends — Coldcard® is a trademark of Coinkite; other names belong to their owners.

The honest part: we don't replace your hot-wallet engine.

High-throughput hot signing — hundreds of withdrawals an hour — is what MPC clusters are built for, and we'll tell you to keep using one there. A hardware signer isn't a certified, high-TPS appliance, and we don't pretend otherwise. What mineracks secures is the **cold and warm tiers — the 95% of reserves and the refill pipe between them**: low-throughput, high-stakes, and exactly where automation with hardware keys you hold beats both a 3am ceremony and a custodian. Cheaper than Fireblocks for the bulk of your funds, and sovereign by construction.

Automate the refill. Hold the keys.

See a live 2-of-3 sign real-signet refills under policy → multisighsm.com

mineracks.com · info@mineracks.com · Brisbane, Australia