SECURING BITCOIN · LUGANO · 22 OCTOBER 2026

You Hold the Keys. Who Holds the Coordination?

The coordination dependencies inside self-custody

Rafael Turon · Founder, Custody Agents · custodyagents.com

ONE SILENCE

This year, keys were born weak and nothing looked wrong.

The secure element held. The supply chain held. The entropy did not, and no screen anywhere said so.

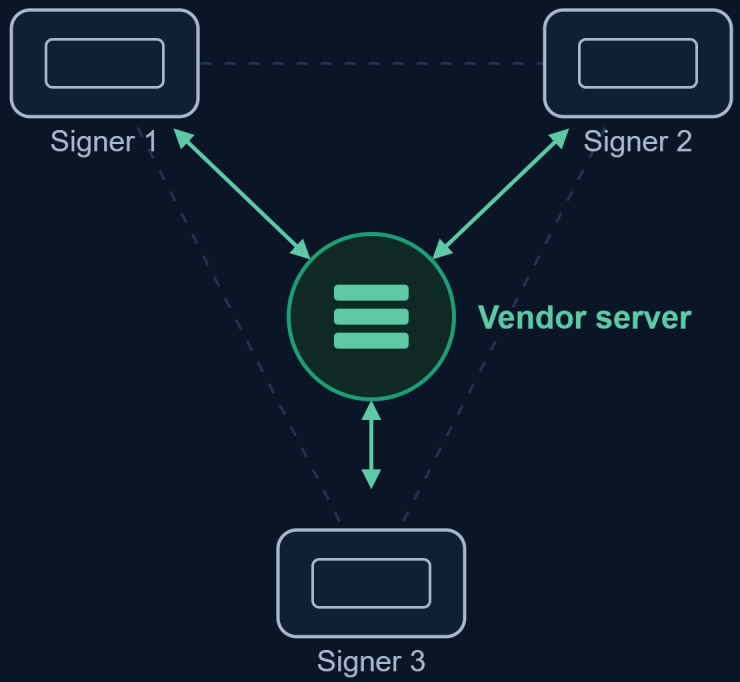
That is the silence this session is about. There is a second one, and it happens every time you spend.

THE SECOND SILENCE

Three keys. Three devices. Descriptors backed up. A modern construction with time-locked recovery paths. Every best practice observed.

Then the owner spends. The wallet builds a PSBT and sends it to a server. The server forwards it to the second signer, collects the signature, passes it back, and eventually broadcasts.

The keys are distributed.
The coordination is not.



Custody Agents · CC BY 4.0

Two independent questions, routinely treated as one

LAYER ONE

Vault construction

Which spending paths exist, under which conditions, enforced by which on-chain mechanism.

Multisig standards, Miniscript, timelocks, the covenant debate. Nearly all of the ecosystem's design attention.

LAYER TWO

Coordination transport

How the people and devices holding shares of those paths exchange the bytes that produce a valid transaction.

Almost none of it.

The two are orthogonal. A brilliant construction can be operated over an observable, censorable transport, and neither layer substitutes for the other.

Custody Agents · CC BY 4.0

What actually travels between signers

BIP-174	PSBT	The transaction itself, moving between signers and accumulating signatures
BIP-327	MuSig2	Two preliminary rounds of nonce exchange, then partial signatures
BIP-129	BSMS	The setup ceremony, agreeing the descriptor before any coins move

Coordination becomes a live question from the second signature onward. A lone single-sig spend needs only broadcast.

Custody Agents · CC BY 4.0

CUSTODY LIFECYCLE ACROSS TWO LAYERS

	SETUP	OPERATION	SETTLEMENT
LAYER ONE **VAULT CONSTRUCTION**	**Descriptor agreement and key exchange BSMS (BIP-129)**	silent by design: the construction does not govern the exchange	**Timelocks and script conditions enforced by consensus**
LAYER TWO **COORDINATION TRANSPORT**	carries the ceremony, claims nothing	**PSBT (BIP-174) MuSig2 nonces and partial signatures (BIP-327)**	out of the picture: the network needs no coordinator

The vault layer owns setup and settlement. The transport layer owns operation, where every transaction actually happens.

Custody Agents · CC BY 4.0

The vendor coordinator concentrates what the script just distributed

Metadata

Who signs, when, in what order, against which descriptor. For a firm or a family, that is the spending graph and the org chart.

Obstruction

It can refuse to forward, or simply be slow. The signers keep their keys and lose their liveness, which under pressure is a freeze.

Fragility

One operator, one point of compromise, one subpoena surface, shared by every customer at the same moment.

None of this violates the on-chain construction. The construction never claimed to govern it.

Custody Agents · CC BY 4.0

WHY EUROPE SHOULD CARE TWICE

Under MiCA, authorisation follows control

Settled

Custody is safekeeping or controlling assets, or the means of access to them, on behalf of clients. Recital 83 keeps providers who neither possess nor control outside the regime.

Open

What control means one layer up from the keys. The regulation does not say, and the coordination path is exactly where the question bites.

Our reading, and I will flag it as a reading: an operator with the standing technical capacity to systematically block or delay a client-initiated transaction is exercising a form of control, whatever the key architecture says.

Custody Agents · CC BY 4.0

RUN THIS ON YOUR OWN SETUP TONIGHT

The coordination fire drill

01 Is your output descriptor saved somewhere your vendor does not control?

02 Can your signers reach each other without that vendor's server?

03 Have you ever completed a spend that way, end to end, on purpose?

Three yeses is operational independence. Two is a plan. One is a story you tell yourself.

Custody Agents · CC BY 4.0

Coordination as a protocol, not as a service

Signers exchange end-to-end encrypted fragments through a mesh of independent relays. No relay holds key material. No relay decrypts what it carries. No relay learns the spending graph, because it cannot tell a nonce from a partial signature from noise.

Assuming the relays are genuinely independent, the worst an adversarial one can do is drop packets.

The community has been probing this since 2022: Joinstr coordinating coinjoin rounds over Nostr relays, Munstr running interactive MuSig sessions across them, Smart Vaults specifying PSBT and policy management on the same substrate, Nunchuk shipping collaborative signing through encrypted relay messages. What the lineage has not yet produced is a formal treatment of the transport itself.

Custody Agents · CC BY 4.0

THE SHARPEST OPEN PROBLEM

Nonce safety under at-least-once delivery

BIP-327 forbids a signer from ever using the same secret nonce in more than one signing attempt. Reuse is not a degradation. It leaks the private key.

The security proof assumes orderly communication. A relay substrate offers the opposite: retries after timeouts, duplicate deliveries, messages arriving out of order, and an adversary who chooses the schedule.

Which invariants the transport must enforce so that uniqueness holds end to end, and proving those invariants sufficient, is open work. Property-based testing finds counterexamples. It does not prove.

Custody Agents · CC BY 4.0

Five problems between a sketch and a specification

- Accountability without a global observer
- Policy-blind transport that still resists garbage
- A threat model sized to eight-figure positions
- Liveness roles when no single server is always online
- **Nonce safety under adversarial delivery**

Stated in public, on Delving, because that is where they should be attacked.

Custody Agents · CC BY 4.0

THE HABIT

Ask both questions. Separately. Every time.

01

What does the on-chain construction guarantee when each key, each participant and each service disappears or turns hostile?

02

What does the coordination path observe, what can it delay, and what fails when it fails?

A vendor with an excellent answer to the first and no answer to the second has described half a security model. So has a vendor in the opposite position.

Custody Agents · CC BY 4.0

M / N

m-of-n was always a statement about authority: how many keys must sign.

It says nothing about how those signatures find each other.

WHERE TO ARGUE WITH THIS

In the open, where it improves fastest

Transport invariants for nonce safety, the working thread

delvingbitcoin.org · topic 2852

Vault Construction and Coordination Transport, with BitVault

intelligence.custodyagents.com/articles/vault-construction-and-coordination-transport

PSBT Coordination over Nostr Relays, the working note

intelligence.custodyagents.com/articles/psbt-over-nostr

DELVING · 2852

Rafael Turon · custodyagents.com · CC BY 4.0 · Criticism of either layer is welcome