POSITION CLARITY · FIELD GUIDE

Wallets and *Custody*

How crypto is actually held, who holds the keys, and what that means for getting at it later. Built for understanding and organizing, not advice. We never ask for your secrets.

Keys Custody Recovery Access

Position Clarity

An educational reference. Made in Canada.

POSITION CLARITY

Contents

01 What owning crypto really means 03

02 The custody spectrum 04

03 Hot versus cold 06

04 The ways people actually lose access 07

05 Custodial versus self-custody 08

06 Mapping your own custody 09

SECTION 01

What owning crypto really means

Owning crypto is not like owning a file on your laptop. You do not really hold coins. You hold the keys that let you move them on a shared record. Once that idea clicks, custody stops being mysterious.

The ledger. A blockchain is a shared record of who owns what, kept by a large network at once. Your coins are entries on that record, not files on your device.

Private key. A long secret number that authorizes moving the coins at an address. Whoever has the private key can move the funds. This is the thing that matters most.

Public address. The shareable destination others send to, a bit like an account number. Safe to share. It reveals nothing that lets someone spend your funds.

Wallet. Not a place that stores coins. It is a tool that stores and uses your keys to read your balance and sign transactions.

Seed phrase, also called a recovery phrase. Usually twelve or twenty-four plain words that can regenerate all the keys in a wallet. It is the master key. Anyone who reads it can take everything.

Not your keys, not your coins

This common phrase has a real point and an honest caveat. The point: if someone else holds the private keys, you are trusting them, not the network, for access. The caveat: holding your own keys is not automatically safer. It moves the responsibility, and the single point of failure, onto you. There is no help desk and no password reset for a lost recovery phrase.

> **THE ONE RULE, STATED EARLY**
>
> Position Clarity never asks for, sees, or stores a seed phrase, private key, or password. Neither should any website, support agent, or person who contacts you. A recovery phrase is typed only into the wallet that created it, never into a website, a form, or a chat.

SECTION 02

The custody spectrum

Custody is who controls the keys. It is not two boxes, custodial or not. It is a spectrum, from a service holding everything for you, to you holding everything yourself. Each step trades convenience for control.

Reading the spectrum. On the left, someone else holds the keys, which is convenient and comes with a reset option, but you rely on them. On the right, you hold the keys, which gives full control and no counterparty, but full responsibility too. A **counterparty** is another party you depend on to deliver. Most people sit somewhere in the middle, often in more than one place at once.

WHERE IT SITS	WHO HOLDS THE KEYS	WHAT TO WATCH
Exchange account	The exchange holds them. You hold a login and a balance, which is a claim on the platform.	*Platform failure, freezes, or account lockout. Your access depends on the company.*
Hosted or managed wallet	A service holds or co-holds the keys on your behalf.	*Convenience with a middle party. Read how recovery and control actually work.*
Hot wallet	You hold the keys, in software on a connected device. **Hot** means connected to the internet.	*Exposure to malware and phishing. Good for small, active amounts.*
Hardware wallet	You hold the keys, on a dedicated offline device. Signing happens on the device.	*Physical loss or damage, and user error. The recovery phrase still rules everything.*
Multisig	Control is split, so several keys are needed to move funds. **Multisig** is short for multi-signature.	*More robust, more complex. More to set up, document, and not lose.*

A crypto ETF is the most hands-off end of all of this. A regulated fund holds the crypto through a professional custodian, and you hold units in a brokerage or registered account. See The Crypto ETF Guide for how that wrapper works.

SECTION 03

Hot versus cold

Two words come up constantly, and they describe one thing: whether the keys touch the internet.

Hot wallet. Keys held on a device that is connected to the internet, such as a phone or browser wallet. Quick to use, and more exposed.

Cold storage. Keys kept offline, away from the internet. Harder to reach for an attacker, and a little slower for you.

Hardware wallet. A small dedicated device that keeps the keys offline and signs transactions on the device itself. The most common way people hold cold storage.

HOT IS GENERALLY GOOD FOR

- Small, active amounts you move often.
- Convenience and speed on a phone or browser.
- Trying things out without much at stake.

WHAT COLD GIVES, AND GIVES UP

- Far less exposure to malware and phishing.
- But it is not a magic shield. Physical loss, damage, and a written recovery phrase are still risks.
- Slower to access, which is the point.

WORTH REMEMBERING Cold storage protects the keys from the internet. It does not protect them from a misplaced device, a damaged backup, or a recovery phrase someone else can read. The phrase is the real master key in every case.

SECTION 04

The ways people actually lose access

Most crypto is not lost to dramatic hacks. It is lost to ordinary gaps. None of the fixes below are products to buy. They are records and habits.

WHAT HAPPENS	WHAT REDUCES THE RISK
The recovery phrase is lost	*A durable backup, kept private, in more than one safe place. Confirm it works before relying on it.*
Locked out of an exchange	*Keep your login method, two-factor backup codes, and the email tied to the account current and recorded privately.*
An exchange fails or freezes	*Know that an exchange balance is a claim on the company. Understand what you hold there versus in your own custody.*
Funds sent to the wrong address	*Most transfers cannot be reversed. Check the address and network, and send a tiny test amount first.*
Phishing or a bad approval	*Treat unexpected links and urgent messages as suspicious. No legitimate party needs your recovery phrase.*
Death or incapacity, no record	*A trusted person can find nothing they do not know exists. This is an organization problem, covered next.*

THE PATTERN

Five of those six are solved by recordkeeping and steady habits, not by buying anything. The sixth, sending to the wrong address, is solved by slowing down. That is most of custody safety.

SECTION 05

Custodial versus self-custody

This is the real fork, and neither side is best at everything. The honest version is a trade, not a winner.

CUSTODIAL, THE CONVENIENT END

- Familiar logins, and a way to recover access.
- Less for you to set up and protect.
- But you do not hold the keys, and you carry counterparty risk if the platform fails.

SELF-CUSTODY, THE CONTROL END

- You hold the keys, with no company between you and your funds.
- No counterparty to fail or freeze you out.
- But full responsibility, and no reset button if the recovery phrase is gone.

Many people use both on purpose. A custodial account or an ETF for convenience and registered-account access, and self-custody for amounts they want to control directly. The point of this guide is not to push you toward either one. It is to make the trade visible, so the choice is yours and the records are ready.

> *Custody is a trade between convenience and control. Name the trade you are making, then write down where things live.*

SECTION 06

Mapping your own custody

Understanding custody is step one. Step two is a calm record of what you hold and where it lives, so you, and the people you trust, are not guessing later. You can do this on paper. It is yours, and it stays with you.

For each holding, record the location, never the secret

RECORD THIS	NEVER RECORD THIS
The asset, roughly how much, and where it lives (which exchange, or which wallet type).	*The seed phrase or private key itself.*
The account it sits in, such as a TFSA, an RRSP, or a personal account.	*Passwords or PINs written in the same place as everything else.*
That a recovery phrase exists, and the general location of the backup.	*The words of the recovery phrase, anywhere digital or shared.*
Who would need to know, and how they would reach a professional.	*Anything you would not want a stranger reading.*

THE BOUNDARY, REPEATED ON PURPOSE

A custody map records where things live and that they exist. It never records the secrets that control them. Position Clarity never sees, requests, or stores any of it. Store recovery material by separate, established methods, and keep your map private.

Educational only. This guide explains how crypto custody works and how to organize a private record of your own. It is not investment, financial, tax, legal, cybersecurity, or estate-planning advice, and it does not tell you what to buy, sell, hold, or use. For decisions about your own situation, consult qualified professionals. Position Clarity never asks for seed phrases, private keys, or passwords.