Your Crypto Shouldn't Die With You

A Practical Guide to Protecting, Recovering, and Inheriting Digital Assets

miras.global

Imagine you pass away tomorrow. Your family knows you own Bitcoin—maybe a lot of it—but nobody knows how to access it. There's no password taped to the fridge, no seed phrase in the filing cabinet, no instructions anywhere. Within hours of your death, your digital wealth becomes a digital tomb: visible on the blockchain, permanently out of reach.

This isn't a hypothetical. Chainalysis estimates that roughly 3.7 million BTC—around 20% of the total supply—are effectively lost. Some of those coins belong to early adopters who threw away old laptops. But a growing share belongs to people who simply died without a plan. Their families are left with nothing: no recourse, no customer service hotline, no court order that can unlock a private key.

The crypto industry has spent a decade perfecting ways to keep assets safe from attackers. It has spent almost no time figuring out how to keep assets safe from *life itself*—from death, illness, accidents, and memory loss. That asymmetry is the gap Miras was designed to close.

This guide covers two things: what to do if you've already lost access to a wallet, and—more importantly—how to set up trustless inheritance so that your digital assets pass to the people you choose, on your terms, without handing control to lawyers, custodians, or centralized platforms.

The Inheritance Gap in Crypto

Traditional finance has centuries of infrastructure for transferring wealth between generations: wills, trusts, probate courts, beneficiary designations on bank accounts. Crypto has none of it. When you hold your own keys, you operate outside the legal and institutional scaffolding that makes inheritance work in the fiat world.

This creates a paradox. Self-custody—the ability to hold assets without relying on banks or intermediaries—is one of crypto's greatest strengths. But it turns into a devastating weakness at the moment of death or incapacitation. A 24-word seed phrase is simultaneously the ultimate expression of financial sovereignty and a single point of failure that can erase a family's wealth overnight.

The numbers tell the story. Between lost passwords, discarded hard drives, and owners who died without sharing access credentials, hundreds of billions of dollars in crypto sits

permanently frozen on-chain. Every one of those locked wallets represents someone's savings, someone's family, someone's plan that never accounted for the unthinkable.

How Crypto Access Gets Lost

Before diving into solutions, it's worth understanding the common failure modes—because most of them are preventable.

Seed Phrases That Vanish

A seed phrase is a 12- or 24-word mnemonic that serves as the master key to a wallet. Lose it, and everything behind it becomes permanently inaccessible. The problem is that seed phrases are analog artifacts in a digital world: they're scribbled on paper, tucked into drawers, and forgotten. House moves, spring cleaning, and well-meaning family members who toss "random notes" account for a significant share of wallet losses.

Industry data suggests that 30–40% of recovery cases trace back to physical media failure—reformatted hard drives, corroded USB sticks, or notebooks that ended up in recycling. The very act of writing something down on paper introduces fragility that most people underestimate.

Passwords Without a Backup Path

There is a critical distinction between a wallet password and a seed phrase. The password protects local access to your wallet app; the seed phrase regenerates the wallet itself. Forget your password but still have the seed phrase? You're fine—just restore the wallet elsewhere. Lose both? Your funds are gone.

Unlike a bank account, there's no "reset password" link. Crypto wallets are designed so that no central authority can override your credentials. That design choice protects you from hackers, but it also means there's no safety net if you forget.

The Custody Blind Spot

Many users don't fully understand the difference between holding crypto on an exchange (custodial) and holding it in their own wallet (self-custodial). On an exchange, recovery is straightforward—just verify your identity. In a self-custodial wallet, recovery depends entirely on you. The phrase "not your keys, not your coins" cuts both ways: if you lose your keys, they're nobody's coins.

Miras addresses this head-on with a 2-of-3 multisig design where no single party—not you, not your heir, not the protocol—can unilaterally move funds. You keep full sovereignty while alive, but there's a trustless fallback that activates only under the right conditions.

Already Locked Out? A Recovery Playbook

If you've lost access right now, here's a practical breakdown by situation.

You Lost Your Password but Have the Seed Phrase

This is the most recoverable scenario. Download the same wallet app you originally used (or any app that supports the BIP-39 standard, which is nearly all of them). Look for "Restore Wallet" or "Import Wallet." Enter your 12 or 24 words in the exact original order—a single transposition generates an entirely different set of keys. The wallet will regenerate your addresses and restore access within minutes.

Once you're back in, set a strong new password with a password manager, and then **set up a Miras inheritance plan** so that next time, even total credential loss doesn't mean total asset loss.

You Lost Your Password to an Exchange Account

Custodial platforms like Coinbase, Binance, and Kraken have standard account recovery flows: password resets via email, identity verification, support tickets. This usually resolves within 24–48 hours.

The catch: your assets sit on someone else's infrastructure. Exchange hacks, insolvencies, and regulatory freezes can all lock you out regardless of your password. **Miras's self-sovereign model avoids this entirely**—you never hand custody to a third party, yet your assets remain inheritable through on-chain smart contracts.

You Lost the Seed Phrase to a Self-Custodial Wallet

This is the hardest scenario. Without the seed phrase, options are slim—but not zero. Before giving up:

- Search every device you owned at the time of wallet creation: .txt files, screenshots, password manager vaults, email drafts, cloud storage.
- Conduct a physical search: notebooks, safe deposit boxes, envelopes in filing cabinets, books you used as bookmark holders, coat pockets, glove compartments.
- Try forensic data recovery tools (Recuva, Disk Drill, TestDisk) on old drives—software wallets often leave traces in specific directories.
- For high-value wallets, reputable recovery firms work on contingency (no recovery, no fee). Beware of scammers—never share your seed phrase with anyone, and reject any firm demanding upfront payment.

Password-cracking tools like BTCRecover can help if you recall fragments of your password. For theft cases, blockchain forensics firms can trace stolen assets and work with exchanges to freeze them.

Miras: Trustless Inheritance for Self-Custodied Crypto

Recovery after the fact is stressful and unreliable. The more intelligent approach is to build inheritance into your setup from day one. **Miras is an open protocol for trustless, non-custodial on-chain inheritance**—powered by Safe multisig wallets and a decentralized network of staked verifiers.

The 2-of-3 Multisig Architecture

When you create a Miras plan, the protocol generates a Safe multisig wallet (the most widely deployed and audited multisig standard in Ethereum). Three keys are created, and no two reside with the same party:

Key	Holder	Role
Key A	You	Day-to-day control of the wallet
Key B	Your heir	Cannot act alone; initiates a claim when needed
Key C	Protocol (encrypted)	Escrowed on-chain; released only after verification

Any transaction requires 2 of 3 signatures. While you're alive and active, you control all operations. Your heir alone cannot touch the funds. The protocol alone cannot touch the funds. **No single party ever has unilateral access.** All key generation happens client-side in your browser—plaintext keys are never transmitted or stored by Miras.

What Happens When a Claim Is Filed

When the time comes, your heir submits a claim on-chain. This triggers three things:

1. **Verifier assignment:** A set of staked verifiers are randomly selected from the Miras network. These are independent participants who've posted financial bonds and face slashing (loss of their stake) if they act dishonestly. Their job: attempt to contact you and confirm whether you're reachable.
2. **Waiting period:** A configurable countdown begins—default is 3 months, but you can set it longer. During this window, if you're alive and well, you simply submit an on-chain objection, and the claim is instantly cancelled. You can also require supplementary evidence like a death certificate.
3. **Quorum release:** If the waiting period expires with no objection and all conditions are satisfied, the protocol's encrypted key (Key C) is decrypted for the valid quorum path. Your heir, holding Key B, now has the second signature needed to move assets. The transfer executes entirely via smart contracts—no intermediary touches the funds.

The Dead Man's Switch

For additional automation, Miras offers an inactivity-based trigger. If you don't interact with your wallet within a timeframe you define, the inheritance process kicks off automatically—no action required from your heir to start the clock.

This is particularly valuable for scenarios where both you and your heir might be unaware of each other's situations—prolonged illness, unexpected incapacitation, or simply life getting in the way. Regular wallet activity resets the timer. But if the silence persists, the protocol interprets it as a signal and begins the verification sequence.

The Heir Readiness Kit

Crypto inheritance fails not just because of technology, but because heirs don't know what to do. Miras addresses this with an optional offline USB guide containing the wallet application, public-facing information, and step-by-step claim instructions. Private keys are never stored in plaintext on the kit. The goal: even an heir with minimal crypto experience can navigate the process.

How Miras Compares

	Traditional Will	Custodial Service	Miras Protocol
You keep self-custody	Yes	No	Yes
No lawyers needed	No	Varies	Yes
Fully trustless	No	No	Yes
Enforced on-chain	No	No	Yes
Heir can't steal early	Depends	Depends	Yes
Protocol can't steal	N/A	No guarantee	Yes
Configurable conditions	Limited	Limited	Yes
Open-source & audited	N/A	Rarely	Yes

Supported Assets

Miras supports **Ethereum (ETH)** natively, plus **Bitcoin (BTC)** via ERC-20 representations—wBTC (custodial wrapped Bitcoin) and tBTC (decentralized, trustless Bitcoin-backed tokens). Any ERC-20 token on supported chains is compatible. For estates spanning multiple heirs, you can create separate Safe wallets per beneficiary or asset bundle, customizing thresholds and allocations independently.

Security Model at a Glance

- **Trustless execution:** Policies, claims, and releases are enforced entirely by smart contracts.

- **Key privacy:** The protocol stores only ciphertext—Key C is encrypted separately with each assigned attestor's public key.
- **Quorum requirement:** No single party can authorize a transaction alone.
- **Incentive alignment:** Verifiers post financial stakes and face slashing for dishonesty.
- **On-chain transparency:** All policy actions are publicly auditable; personal data stays off-chain.
- **Open source:** The codebase is public and the platform has undergone security audits. Patent Pending 63/914,518.

Complementary Best Practices

Miras handles the inheritance layer, but defense in depth means pairing it with solid personal security habits.

Redundant Seed Phrase Storage

Even with Miras in place, maintain at least three copies of your seed phrase in geographically separate locations. Write them on durable materials—stamped steel plates or titanium capsules survive fire, flood, and decades of neglect. For an extra layer of safety, consider a Shamir Secret Sharing scheme that splits the phrase into “shares” requiring a minimum threshold to reconstruct.

Password Hygiene and 2FA

Use a reputable password manager (Bitwarden, 1Password, or similar) to generate and store strong, unique credentials. Layer on two-factor authentication everywhere—preferably a hardware key like YubiKey, or at minimum an authenticator app. SMS-based 2FA is better than nothing but remains vulnerable to SIM-swap attacks.

Device and Network Security

Install reputable antivirus and VPN software on every device that touches your crypto. Phishing malware can silently capture seed phrases from clipboard or screen. For hardware wallets, buy only from the manufacturer or authorized dealers—never from third-party marketplace sellers—and verify tamper-evident packaging on arrival.

Practice Your Recovery

Every six months, run a recovery drill: restore a test wallet from your backup seed phrase using a small amount of funds. This validates that your backups are intact and keeps the process fresh in your memory for when it actually matters.

Estate Planning with Miras

Traditional crypto estate planning—sealed envelopes with seed phrases, instructions filed with an attorney—is fragile. Lawyers may not understand crypto. Family members may mishandle private keys. Envelopes can be lost or opened prematurely.

Miras replaces these analog workarounds with programmable, on-chain enforcement. Your inheritance plan is encoded in smart contracts that execute automatically when conditions are met. You can still maintain a written inventory of your holdings for your heirs’ reference, but the actual transfer mechanism is trustless: claim, verification, waiting period, quorum release. No probate court, no executor discretion, no ambiguity.

For complex estates, Miras supports multiple heirs via separate Safe wallets, configurable waiting periods per beneficiary, additional documentation requirements

(death certificates, notarized proof), and higher quorum thresholds (e.g., 3-of-5) for extra security on large holdings.

Avoiding Recovery Scams

Desperation makes people vulnerable, and the crypto space has no shortage of predators targeting those who've lost wallet access. A few ground rules:

- **Contingency only:** Any legitimate recovery firm charges a percentage of recovered assets—never an upfront fee.
- **Ignore cold outreach:** Scammers monitor social media for people discussing lost wallets. Reputable firms don't send unsolicited DMs.
- **Verify independently:** Look for a real business address, documented recoveries, and reviews on multiple third-party platforms.
- **Your seed phrase is sacred:** No legitimate service will ever ask for it. Full stop.

With Miras, the need for third-party recovery services largely disappears. Your inheritance plan is encoded on-chain—there's no middleman to trust, no "recovery specialist" to vet, and no window for social engineering.

Under the Hood: How the Cryptography Works

For those who want to understand the mechanics:

A seed phrase follows the BIP-39 standard, converting a random number into a human-readable mnemonic drawn from a fixed list of 2,048 words. The word order encodes a master private key; a final checksum word validates the sequence's integrity. From this master key, all wallet addresses are deterministically derived. Change one word or swap two positions, and you get an entirely different wallet.

Miras builds on top of Safe (formerly Gnosis Safe), the most battle-tested multisig infrastructure in the Ethereum ecosystem, securing tens of billions in assets. Instead of concentrating everything behind a single seed phrase—a catastrophic single point of failure—Miras distributes control across a multi-signature quorum.

Key C is generated entirely in the user's browser, encrypted client-side, and stored as ciphertext on Ethereum. Each assigned attestor receives a copy encrypted with their own public key, so only they can decrypt their share. Your Safe address and contact details follow the same encryption model—the protocol never sees plaintext.

This architecture means that even if one key is compromised, an attacker still needs a second key from an independent source. And unlike raw seed-phrase recovery, Miras adds a human-verifiable safety layer—the verification period and staked verifiers—on top of the cryptographic guarantees.

The Road Ahead

The crypto industry has experimented with social recovery wallets, multi-party computation, and biometric authentication. Each represents progress. But none of them solve inheritance in a trustless, fully on-chain way that preserves self-sovereignty.

Miras occupies a unique position: it's not asking you to choose between security and recoverability, or between self-custody and peace of mind. It encodes your wishes into blockchain code—programmable, auditable, and free from the discretion of any third party. Time-based triggers, configurable quorums, and staked verification create an inheritance layer that's as trustless as the assets it protects.

The billions in permanently frozen crypto are a monument to a problem the industry ignored for too long. Miras is the infrastructure that ensures the next generation of crypto holders doesn't repeat the same mistake.

Your Next Steps

If you're currently locked out, follow the recovery playbook above. Don't give up—document everything you remember about your wallet setup, passwords, and where you might have stored backups.

If you still have access to your wallets, act now:

1. **Set up a Miras inheritance plan** at miras.global so your assets have a trustless path to your chosen heirs.
2. Create durable physical backups of your seed phrase (steel or titanium) and store copies in at least three separate locations.
3. Move significant holdings to a hardware wallet purchased directly from the manufacturer.
4. Enable hardware-key 2FA and use a password manager for every crypto-related account.
5. Share the Miras Heir Readiness Kit with your designated heir so they know exactly what to do.

The goal isn't perfect security—it's layered protection that makes loss nearly impossible and inheritance automatic. With Miras, you get **full control today and trustless succession tomorrow.**

Frequently Asked Questions

Q: My family member died and held crypto. Can Miras help retroactively?

A: Only if the deceased had already set up a Miras plan. The protocol works by pre-configuring a multisig wallet and key distribution while the user is alive. If no plan was established, you're limited to traditional recovery methods—searching for seed phrases, engaging forensic recovery firms, or working with custodial exchanges where the deceased held accounts. This is exactly why setting up Miras proactively matters.

Q: How is Miras different from just writing my seed phrase in my will?

A: A seed phrase in a will gives whoever reads it—the attorney, the executor, a courthouse clerk—full, immediate control over your funds. It can be stolen, mishandled, or leaked long before it reaches your heir. Miras distributes control across a 2-of-3 multisig: your heir holds only Key B, which is useless without Key C. Key C is only released after a verified waiting period with no objection from you. There's no moment where a single document or person holds complete access.

Q: What stops my heir from filing a false claim while I'm alive?

A: Multiple layers. First, the configurable waiting period (3 months by default, longer if you choose) gives you ample time to notice. Second, staked verifiers actively try to contact you. Third, a single on-chain objection from you cancels the claim immediately. Fourth, dishonest verifiers lose their financial stake through slashing. The system is designed so that a false claim is both difficult to execute and expensive to attempt.

Q: Can the Miras protocol itself access my funds?

A: No. The protocol holds only an encrypted copy of Key C—one key in a 2-of-3 multisig. Moving funds requires two keys. Since the protocol controls only one (and only in encrypted form), it can never authorize a transaction on its own. The code is open-source, so this guarantee is independently verifiable.

Q: What assets does Miras support?

A: Ethereum (ETH) and all ERC-20 tokens natively. Bitcoin (BTC) is supported through ERC-20 representations: wBTC (custodial wrapped Bitcoin) and tBTC (decentralized, trustless Bitcoin-backed tokens).

Q: Can I set up inheritance for multiple heirs?

A: Yes. Create separate Safe wallets per heir or per asset bundle. Each wallet can have its own threshold, waiting period, and documentation requirements. This lets you allocate specific assets to specific people while keeping risk isolated.

Q: How long does the claim process take?

A: The default waiting period is 3 months, which you can extend when configuring your plan. This timeframe balances protection against false claims with practical timelines for legitimate inheritance. If you still have your seed phrase, standard wallet recovery (separate from Miras) takes under 10 minutes.

Q: What if quantum computing breaks current encryption?

A: Quantum computers capable of breaking elliptic-curve cryptography are still estimated to be years or decades away. When they arrive, both Ethereum and Miras will migrate to post-quantum algorithms—this is an industry-wide challenge, not specific to any one protocol. In the meantime, a properly configured inheritance plan is your best protection against all other, far more likely, failure modes.

Q: Is the Miras codebase auditable?

A: Yes. Miras is open-source and has been security-audited. Anyone can inspect the smart contracts, verify the multisig logic, and confirm that the protocol behaves as documented. Transparency is a core design principle.

Your Digital Legacy Deserves a Plan

Set up trustless, non-custodial crypto inheritance in minutes.

Get started at **miras.global**