FIRM6102

# Bitcoin Continuity Field Memo

Quarter: Q1 2026 | Version 2.1

## Executive Summary

We're seeing a new premium client segment emerge inside CPA firms: self-custody Bitcoin holders with meaningful exposure. The risk profile is different from traditional assets because Bitcoin is a bearer asset—control is operational, not just legal. Most families have security tactics, but very few have continuity: a plan that survives death, incapacity, and the slow decay of keyholders and procedures over time. This memo summarizes what breaks first, what holds up, and a simple screen CPAs can use to identify continuity-critical clients without becoming technical experts.

## Signals: How to Spot These Clients in Your Book

You likely already have them. Watch for these three patterns:

- **Bitcoin is material vs. liquid net worth.** Holdings represent a significant portion of the client's liquid wealth.
- **"Can we put this in the trust?" or "What happens if I die?"** These questions signal the client is thinking about continuity but doesn't have a plan.
- **Holdings are fragmented.** Bitcoin sits across exchange accounts, hardware wallets, mobile wallets, and "misc wallets" with no unified map.

## The One Big Pattern: From "Owning" to "Governing"

The most sophisticated clients are no longer just "owning" Bitcoin; they are building systems to govern it. As holdings grow and setups become more complex (often a mix of exchange accounts, hardware wallets, and trust structures), the primary risk shifts from price volatility to continuity failure. Tax returns don’t fail—access and operational control fails. This creates a recurring advisory

opportunity for the CPA firm that can quarterback the process, align the legal and technical layers, and ensure the client's plan remains resilient year after year.

## Where Setups Fail: Common Break Points

These are the most common failure modes we see in the field. They represent a gap between a client's intentions and the operational reality of their setup.

- **Exchange-Heavy Custody:** Relies on a single institution, creating access bottlenecks at death or incapacity due to 2FA and account control issues.
- **Single-Seed Wallet:** A single point of failure where the loss or discovery of one seed phrase can compromise the entire holding, with no recourse.
- **"Paper Trust" Only:** The legal language exists in a trust document, but there is no corresponding operational recovery plan for the trustee to execute.
- **Multisig Without Governance:** The technical setup is in place, but keyholders drift, no drills are performed, and there is no defined logic for replacing a lost or unavailable keyholder.
- **Fragmented Basis & Records:** Exchange exports, wallet transfers, and prior-year gaps make audits and estate administration slow and expensive.

> **So what:** Most clients have security tactics, but they lack a durable continuity operating system. Their plans are brittle and likely to fail under stress.

## What Works: The Resilient Operating System

The most durable continuity plans are not one-time fixes; they are living systems built on a few repeatable components. These elements work together to ensure control can be maintained and transferred reliably over time.

- **A Written Continuity Map:** A clear document outlining all assets, roles, key custody arrangements, and recovery paths.
- **An Aligned Control Layer:** The technical setup (e.g., multisig) actually matches the roles and permissions described in the legal documents.
- **Annual Drills & "Break Glass" Tests:** Regular, structured walkthroughs of recovery procedures to ensure they work and keyholders are prepared.

- **Active Keyholder Governance:** A defined process for check-ins with keyholders and a clear protocol for replacing them if one becomes unavailable.

> **So what:** The best outcomes come from aligning the legal structure with the operational reality and then drilling it annually. The CPA is the natural hub for this process.

### Client-Facing Explanation (Forwardable)

Bitcoin is a bearer asset. A trust or will can say who should inherit it, but that doesn't automatically give them the ability to access it. Continuity means your legal plan and your access plan match—and that you test it periodically.

## The Tool: 5 Questions to Identify Continuity-Critical Clients

If the answer is "No" or "Not sure" to any of these questions, the client has a critical continuity risk that needs to be addressed. This screen allows you to flag at-risk clients in minutes, without needing to be a technical expert.

1. If you were unavailable for 30 days, could your spouse or trustee access your Bitcoin without guessing?
2. Is there a written map of who can access it and how?
3. Have you tested recovery in the last 12 months?
4. If a keyholder (the person holding a key or access credential) becomes unavailable or uncooperative, is there a defined process to replace them?
5. Are your tax and basis records organized well enough to survive an audit or estate administration without your involvement?

## The Next Step: A Low-Friction Workflow

The goal is not to become a Bitcoin custody expert, but to own the client relationship and quarterback the solution. By using the 5-question screen, you can flag high-risk clients and introduce a simple, low-friction workflow: **Identify** the risk, **Triage** the weak points with a continuity checkup, help the client **Fix** the gaps by coordinating with legal and technical experts, and **Maintain** the plan with an annual review. This protects your client, mitigates firm risk, and opens a new, high-value retainer lane of recurring advisory revenue.

---



**Fitzgerald Hall**

**Founder, Firm6102**