Ledger Continuity — Service Overview v1

Treasury continuity intelligence for crypto-native organizations with stablecoin, custody, chain, bridge, counterparty, and yield exposure.

What problem this solves

Crypto-native treasuries often look diversified until one dependency fails. A team may hold funds across exchanges, custodians, chains, bridges, wallets, and yield venues, while still relying on one issuer, one redemption path, one signer group, one payment rail, or one emergency decision process.

Ledger Continuity helps leadership answer:

> If a stablecoin, custodian, exchange, chain, bridge, counterparty, or yield venue fails under stress, can the organization still operate?

Who it is for

• DAO treasuries and foundations managing runway, grants, reserves, or incentive programs.

• Crypto startups with meaningful stablecoin runway, vendor, payroll, or customer settlement exposure.

• CFOs, treasury managers, and operators who need a board-readable risk and continuity artifact.

• Stablecoin/payment operators preparing for launch, partner review, or operational scale.

• Funds/platform teams supporting portfolio-company treasury decisions.

What a review includes

• Executive dashboard and Treasury Continuity Score.

• Exposure map by asset, issuer, chain, venue, custodian, purpose, and owner.

• Critical/material risk table.

• Largest single failure point.

• Board-facing heatmap.

• Operating Cash / Settlement Liquidity / Risk-Return bucket analysis.

• Recovery readiness assessment.

• Governance escalation matrix.

• Incident-response playbook.

• Source hierarchy, confidence labels, and freshness labels.

• Privacy/no-wallet/no-custody boundary.

What this is not

This is not financial advice, investment advice, legal advice, tax advice, accounting advice, compliance advice, security audit, asset management, custody, trading, transaction execution, or wallet access.

Typical output

A board-forwardable memo/package that shows what could break, why it matters, what evidence supports each finding, what is unknown, and what management should verify next.

Useful client inputs

No private keys, seed phrases, signing authority, custody access, or transaction permissions are requested.

Useful inputs include stablecoin exposure ranges, chains, token versions, custodians, exchanges, wallets, payment flows, yield venues, approval process, deadlines, and known concerns. Anonymized exposure structures are acceptable for early review.