Is Your Agency Ready for Crypto Seizures?

Key Takeaways

The Limits of Consumer Tools

Hardware wallets and exchanges were built for retail users, not law enforcement. Three structural limits: no record of who moved what, no protection once a seed phrase has been seen, and no support for every chain a case may involve.

Security Is Not a Policy

A policy requiring two officers can be written, signed, and bypassed by anyone with system access. Security is programmatic, not a guideline. When controls are enforced by software rather than judgment, compliance becomes the default.

One Person is Not a Strategy

When a single officer holds the seed phrases, workflows, and institutional knowledge, the entire capability leaves with them. The fix is not simply hiring more specialists. It is using software that encodes the workflow, so technical expertise is no longer a single point of failure.

Build the Infrastructure First

Building the infrastructure before opening crypto seizures to wider use feels slow at first. **The trade-off is moving faster and with greater confidence later** - on real software and process, not sticky notes and one-off workarounds as case volume grows.

Liquidation Is an Underestimated Process

Returning seized crypto to a victim is multi-step: liquidate through a law enforcement exchange account, cash out to a separate bank, and route through state treasury before a check issues. The conversion phase deserves planning, not improvisation at the end of a case.

Audit the Action, Not Just the Asset

Chain of custody for digital assets is not about where the asset is stored, it is about who acted on it and when. A locked safe says the asset is secure; it does not say who touched it. That distinction is what makes a case defensible in court.

asset reality

Ready to see the platform?
Scan the code to find out more

The Readiness Checklist

Use the following checklist to assess your agency's current state of readiness for crypto asset seizures. Each item is intended to be answered with a yes or no, supported by evidence the agency could produce on request. Items that cannot be confirmed represent gaps to address with command staff, the prosecutor's office, and the officers responsible for handling seized assets.

- ☐ Credentials are stored in a secure location with documented access for designated backups.
- ☐ Critical workflows (transfers, approvals, access changes) are enforced by software controls, not policy alone.
- ☐ Every action on a seized asset is logged automatically with user, action, and timestamp.
- ☐ A current inventory of every wallet, exchange account, and tool exists, including supported chains and tokens.
- ☐ Custody infrastructure covers every asset type with no minimum value requirement, and wallet addresses can be secured in real time to avoid asset loss.
- ☐ Rollout is phased across units and case types, gated on infrastructure readiness, not case volume.
- ☐ A defined liquidation process names owners for fiat conversion, reconciliation, treasury transfer, and victim restitution.
- ☐ The audit trail for every seized asset is system-generated, independent of any investigator's notes or memory.
- ☐ Chain of custody would withstand cross-examination today, identifying everyone who accessed or moved the asset.