

JANUARY 29, 2024



DIGITAL ASSET STRATEGIC SERVICES

A COMPREHENSIVE SYSTEM FOR FEDERAL AGENCIES TO TAKE POSSESSION
AND SAFE CUSTODY OF CRYPTOCURRENCIES AND OTHER DIGITAL ASSETS

KEITH LAWHORN
ENVARIAN
info@envarian.com



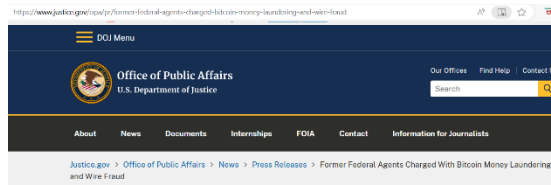
This system offers a set of products and services, as well as training and procedures that will guide federal agencies in the successful seizure, custody, and maintenance of digital assets. From safely taking possession to documentation for later analysis, this system will help ensure that industry best practices are available to your employees.

Introduction

The rapidly emerging, constantly rapidly emerging, constantly changing, and complex world of new digital assets is offering a new challenge to the law enforcement community.

Addressing these challenges will take an agency-wide approach and new standards.

The challenges are real, as seen below:



News PRESS RELEASE
All News
Blogs
Photo Galleries

Former Federal Agents Charged With Bitcoin Money Laundering and Wire Fraud



Digital frontier: A technology deficit in the boardroom

The Deloitte Global Boardroom Program's new research of directors and corporate leaders reveals underinvestment in technology and uncovers gaps in board engagement on digital transformation

Upcoming Challenges:



USDA: Amish Dairy Farmers busted in crypto-raw milk exchange ring.

12/15/2030

According to unnamed sources, the USDA has recovered over \$2 million in Bitcoin and raw milk in a multi-state sting operation.



Will your Agents understand the next steps?

Offerings

Services: Digital Asset Strategy Service (DASS) – 24/7, audited and monitored crypto test lab capable of assisting in digital asset transfers. This service would include predefined or real-time secure private key generation, without the need for third-party custody (i.e., emergency crypto transfers without leaving Federal custody). Test-net blockchain environments hosted for all major platforms.

Service: Digital Asset Monitoring Service (DAMS) – real-time automated monitoring and Alert System. This system will offer immediate alerts to an agency regarding any transactions related to a public key address. In other words, this system will monitor any wallet for real-time transactions. The system will offer an API to the agency allowing for integration to existing systems.

Product: Training and field manuals on the discovery, possession, and safe custody of digital assets for field officers. Such as:

- **Digital wallet identification**, including step-by-step tutorials for all major platforms.
- **Documenting wallet** addresses and transactions.
- **Discovering hard-to-find assets.**
- **Designing a cryptocurrency test lab**, including setting up online and well as off-line wallets. Establishing a trusted blockchain explorer list.
- Recommendations for **private key vaulting solutions** or interacting with third-party custodians.
- Field Agent's **Guide to Digital Asset Seizure** and Documentation.
- **Understanding blockchains**, transactions and confirmations.
- Digital Assets **Forensic Analysis, UTXOs and transaction manipulation** for purposes of obfuscation, as well as, assembling unrelated transactions.
- Off-line solutions for signing transactions in an **air-gapped environment.**
- **Reading the Blockchain** – a deep dive into the blockchain, transaction assembly, transactions in memory, resolving failed or stalled transactions, and much more.
- **Asset Transfer Planning** – developing asset transfer strategies, to prevent monitoring or disruption from third parties and subjects of investigations.
- **Security By Obscurity** – a planning guide for avoiding surveillance detection, re-directing your crypto transactions to obscure the ultimate destination address. Address consolidation, UTXO management, transaction fee management, block-assembly strategies and more.

- ◆ **Product: Crypto-Discoverer** - A browser-based Agency-deployed intranet application offering a click-through guide identifying various ways cryptocurrencies may be stored. How to determine if exigency exists regarding necessary transfers (i.e., how would a field agent determine if the assets are at risk of being lost or stolen). What to do when a transaction fails. When should a field agent NOT move cryptos; some circumstances require prior forensic analysis. When would taking immediate action harm a potential investigation. The default workflow would follow industry best practices; however, customization could be offered for specific methods and policy guidelines.

- ◆ **Product: Crypto-Explorer** – A set of private keys or a seed phrase may be used by single wallet or device, however, there is almost limit to the number of public addresses that could be accessed. For example, if a wallet uses a 12-word seed phrase and a cryptographic algorithm with 128 bits of entropy, the total number of possible wallets is approximately 3.4×10^{38} wallets, an enormous number. There is no possible way of knowing how many assets are stored on a set of private keys without an automated process of discovery. Discovery requires real-time Blockchain analysis, as well as an understanding of Layer 1, Layer 2, and cross-chain protocols. Understanding side-chain protocols, unsettled transactions, and mainnet transactions. Our solution automatically scans all major cryptocurrencies and Digital Asset platforms to identify standard protocol public addresses and report asset inventories for any set of private keys or seed phrase passwords.

- **Service: Emergency Digital Assets Service (EDAS)** - A best-effort service for emergency digital asset storage in the event an agency cannot take custody using their own resources. This should include a Multi-signature wallet solution, such that spend transactions would require the agency to authorize transactions.

These offering could include third-party custodians on behalf of the agency.

- An add-on service could offer solutions when the digital asset is not available to a US-based custody provider.
- An additional service could be public key address analysis and digital asset inventory; including hard-to find assets such as NFTs stored inside a layer-2 protocol; unsettled side-chain transactions; identify potential third-parties or trustees in possession or holding portions of a Multi-Signature key. Advise on transaction management including designing the best approach to transact highly fragmented wallet addresses, choosing the right transaction fees for exigent circumstances.

