TRM

Common Crypto Artifacts and Their Role in Investigations

How to spot hardware and software wallets, apps, phrases, keys, and other digital evidence of crypto activity

Hardware wallets

What is a hardware wallet?

Hardware wallets are physical devices designed to securely store cryptocurrency private keys offline. These devices isolate private keys from internet-connected systems and require user authentication – typically via a PIN, passphrase, or biometric input. Some include touch screens or physical buttons to approve transactions, and may resemble small remotes, credit cards, or other portable electronic devices.

Why is it important to identify hardware wallets?

Hardware wallets are commonly used by travelers to securely store and access their cryptocurrency holdings. The device itself contains the private keys necessary to authorize transactions, effectively serving as the gateway to the user's digital assets.

While hardware wallets do not store transaction history, connecting them to their companion software can reveal wallet balances and transaction records by querying the blockchain. If a hardware wallet is unlocked or its PIN/passphrase is known, border security officers may be able to access the associated cryptocurrency.

Hardware wallets can be categorized as either Bitcoin-only or multi-coin devices. Bitcoin-only wallets are designed exclusively for Bitcoin, whereas multi-coin wallets support a variety of cryptocurrencies.

These devices are typically protected by a PIN, passphrase, or both. An unlocked hardware wallet should be treated as sensitive, high-value potential evidence and handled strictly in accordance with your agency's digital asset protocols. Improper handling risks irreversible loss of access to cryptocurrency funds, or compromise of evidentiary integrity.

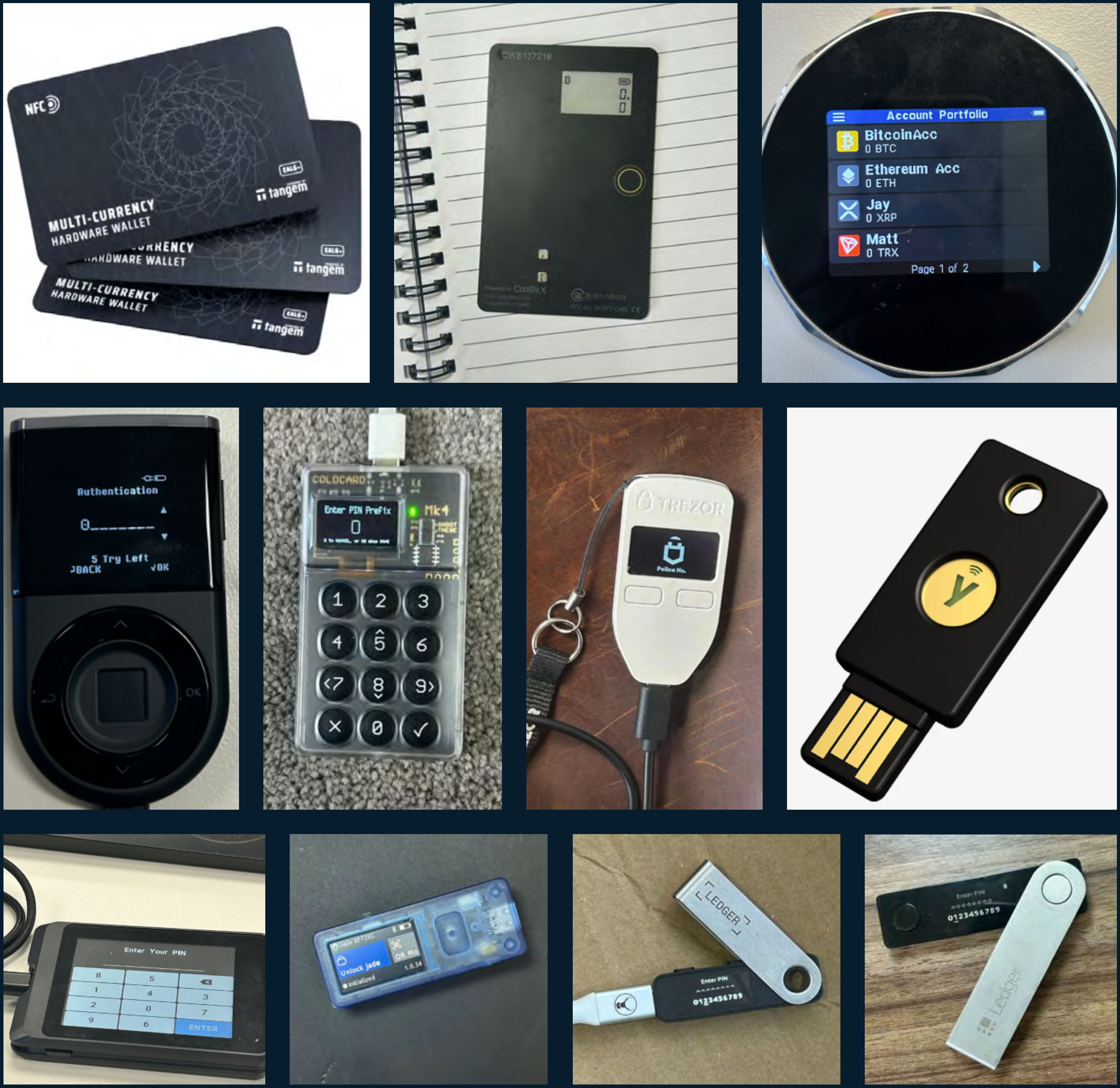
Where are hardware wallets typically concealed?

Due to their compact size and unassuming appearance, hardware wallets can be concealed in various ways by travelers. While common locations include pockets, wallets, or money belts, they may also be stored in carry-on luggage or hidden within everyday items such as travel pillows, shoes, or toiletry bags. Given these concealment methods, thorough and attentive inspections are essential to identify and secure these devices.

Sample questions to ask

- **Do you use hardware wallets?**
- **Which hardware wallet do you use? Is it with you now?**
- **Do you have the seed phrase or private key for your wallet?**
- **Do you use a PIN, code, passphrase, or password to access your wallet?**
- **Does anyone else have access to the seed phrase or private key for your hardware wallet?**
- **Do you use software on a phone, tablet, or laptop to access your wallet?**
- **Do you have this software installed on any of your electronic devices with you now?**

Hardware wallets



Software wallets and apps

What is a software wallet?

Software wallets are digital applications run on internet-connected devices – including smartphones, laptops, and desktops – that store cryptocurrency private keys locally. These wallets may appear as mobile apps (e.g. Trust Wallet), desktop programs (e.g. Exodus), or browser extensions (e.g. MetaMask, Rabby).

Travelers use software wallets to quickly access, send, and manage virtual assets from personal devices. These wallets often connect directly to cryptocurrency exchanges or decentralized applications. A single device may host multiple wallets across mobile apps and browser extensions, with each wallet potentially tied to separate accounts, networks, or currencies.

Officers should treat any device with a software wallet as a potential access point to active cryptocurrency holdings. These wallets often support multiple assets, may auto-sync with online accounts, and can be secured using passwords, biometrics, or two-factor authentication (2FA).

Why is it important to identify software wallets and apps?

The presence of exchange platforms or software wallet apps on a traveler's device is a key indicator of active or recent cryptocurrency use, and should immediately prompt deeper questioning. These apps may signal undeclared digital assets crossing the border, provide insight into the traveler's financial behavior, and help assess the sophistication of their crypto activity. If the device is unlocked or the apps are accessible, officers may gain real-time visibility into wallet balances, linked bank accounts, and transaction history. This type of access is high-value: it supports seizure decisions, strengthens evidentiary documentation, and generates actionable intelligence for broader investigations.

Peer-to-peer payment apps like Venmo, PayPal, and CashApp also support various built-in cryptocurrency features, allowing users to buy, sell, and hold assets like Bitcoin and Ethereum directly within the app. Crypto activity in these apps may represent undeclared assets, especially if values exceed reporting thresholds, like USD 10,000 in BTC in PayPal. Because accounts are linked to real-world identities (via KYC), these apps also offer useful attribution leads.

The presence of both crypto-native apps (e.g. MetaMask) and fiat-to-crypto P2P apps (e.g. CashApp) on the same device may indicate hybrid use – including attempts to off-ramp, launder, or conceal assets. Officers should treat P2P apps as potential crypto indicators and review transaction logs, balances, and linked accounts when accessible.

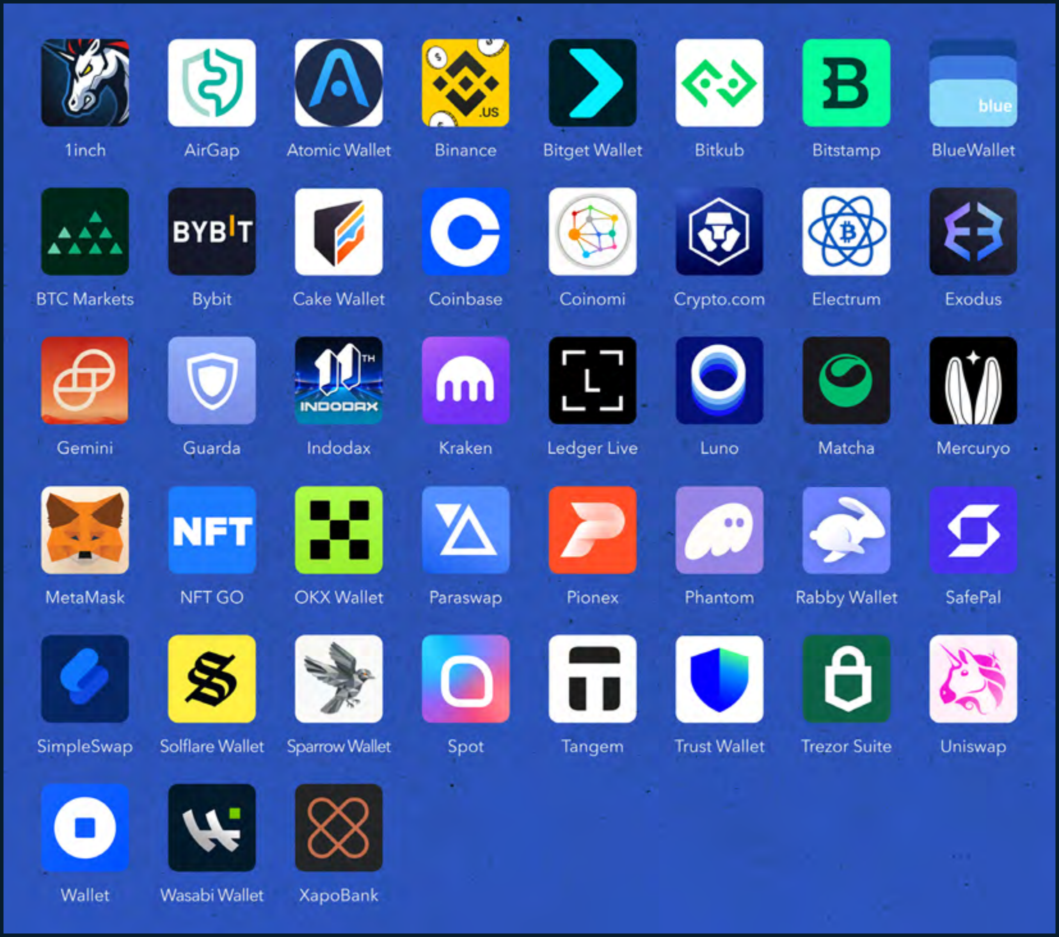
Why is it important to identify software wallets and apps?

Software wallets and crypto-related apps may be visible on any screen or within the app drawer of smartphones, but are often hidden in folders, secured with app locks, or stored in private areas (e.g. Secure Folder on Android, App Library on iOS). On laptops, wallets may appear as standalone programs (e.g. Exodus, Atomic Wallet) or as browser extensions (e.g. MetaMask, Rabby). Officers should check browser extension menus, file directories (e.g. Downloads, AppData, Applications), and pinned taskbar apps. Access is commonly protected by passcodes, biometrics, or multi-factor authentication.

Software wallets and apps

Sample questions to ask

- Do you use software wallets?
- Which software wallet(s) do you use? Is it / are they installed on any of the devices with you now?
- Do you have the seed phrase or private key for your wallet?
- Is your software wallet unlocked?
- Do you use a PIN, code, passphrase, or password to access your wallet?
- Do you use a hardware security device, such as a YubiKey, to access your wallet?
- Does anyone else have access to the seed phrase or private key for your hardware wallet?



Seed phrases and private keys

What is a seed phrase or private key?

A seed phrase is a human-readable string, most often 12–24 randomly generated words, used to back up and regenerate a master private key. That master key is then used to derive all associated wallet addresses and private keys within a cryptocurrency wallet.

In some cases, seed phrases may be abbreviated, with only the first four letters of each word written down (e.g. abou aban acce accu instead of about abandon access account). This works because the BIP39 wordlist is designed so that the first four letters of each word are unique, allowing wallet software to reliably auto-complete and validate the full phrase.

Some wallets like Electrum support custom or non-standard seed formats, including short phrases or minimal inputs that don't follow the typical 12–24 word BIP39 structure.

Why is it important to identify seed phrases and private keys?

Possession of a traveler's seed phrase enables border officers or investigators to recover the entire wallet, including access to potentially hundreds of addresses and associated cryptocurrency funds. Even a single private key may grant access to funds at one address. Both seed phrases and private keys should be treated as high-value evidence and handled in accordance with your agency's digital asset procedures.

This emphasizes the critical importance of proper handling procedures to maintain both access to digital assets and the integrity of the evidence. Because a seed phrase can be used to recreate a wallet on another device and immediately move funds out, possession of a seed phrase is equivalent to possession of the assets themselves. Mishandling or delay in securing seed phrases may result in irreversible loss of access to the assets, as they can be quickly transferred beyond investigative reach.

Where are seed phrases and private keys typically concealed?

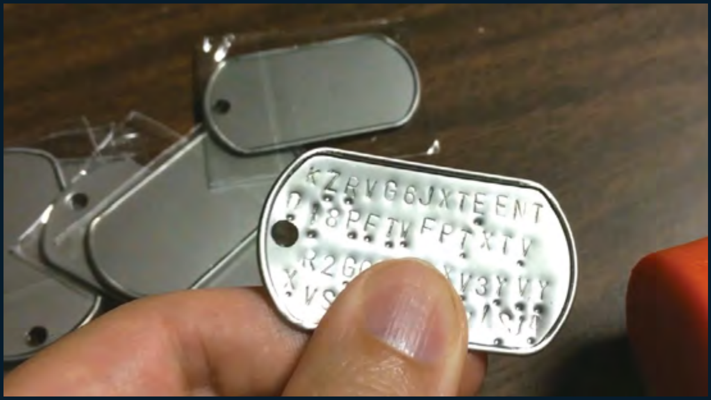
Seed phrases and private keys, which serve as direct access to a traveler's cryptocurrency, may be stored in both digital and physical formats. Digitally, they are often saved in photo libraries, cloud drives, notes apps, password managers, text messages, or file folders on a traveler's electronic device. Wallet passwords may be stored in a password management app (e.g. 1Password, LastPass, or Keeper). And private keys may be in the form of QR codes, because they consist of a long series of letters and numbers, which can be difficult to remember.

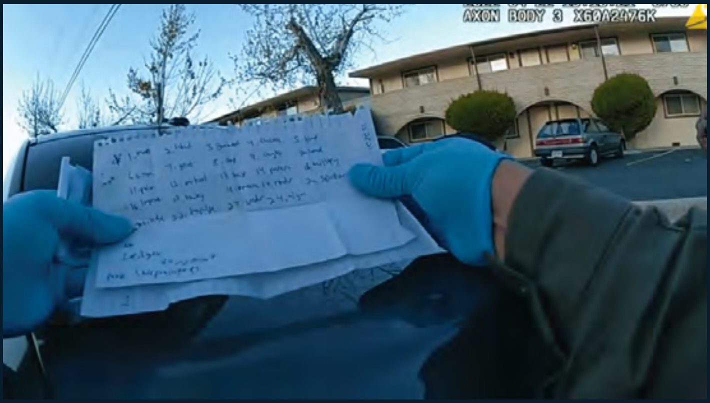
Physically, seed phrases and private keys may be written down or printed on small cards resembling credit cards that display the seed phrase, private key, or a QR code representation. These may also appear on notebook pages, hardware wallet backup cards, or scrap paper. Some travelers may store seed phrases in metal crypto safes designed to withstand fire, water, and physical damage, such as the Cryptosteel Capsule or Billfodl.

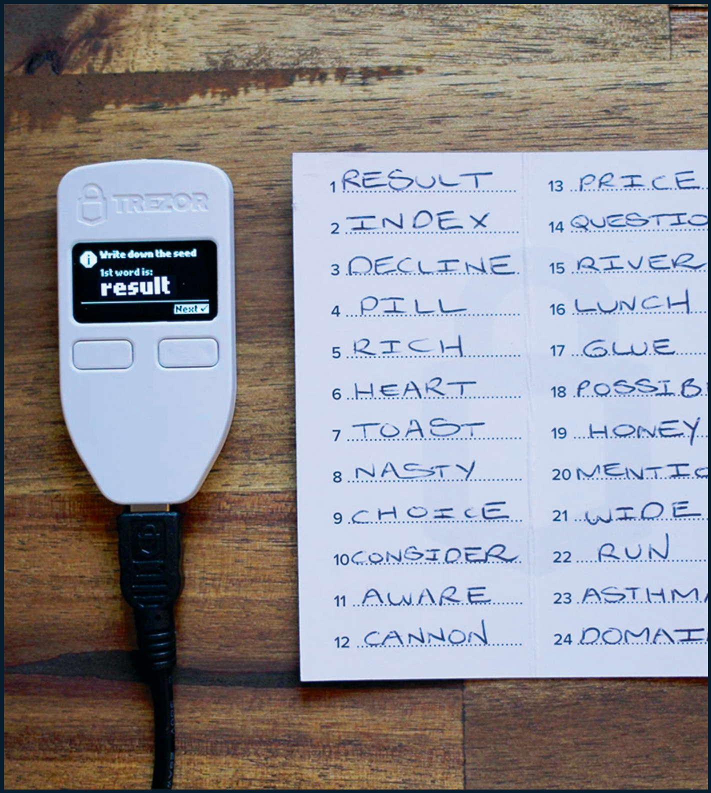
Sample questions to ask

- **Do you use hardware or software crypto wallets?**
- **Do you have the seed phrase or private key for your wallet?**
- **Do you use a password to access your wallet?**
- **Does anyone else have access to your seed phrase or private key?**
- **Where do you keep your seed phrase, private key, or password?**
- **Has anyone shared their seed phrase or private key with you?**

Seed phrases and private keys







Write down the seed
1st word is:
result
Next

1 RESULT
2 INDEX
3 DECLINE
4 PILL
5 RICH
6 HEART
7 TOAST
8 NASTY
9 CHOICE
10 CONSIDER
11 AWARE
12 CANNON
13 PRICE
14 QUESTIO
15 RIVER
16 LUNCH
17 GLUE
18 POSSIB
19 HONEY
20 MENTIO
21 WIDE
22 RUN
23 ASTHM
24 DOMAI

1 BASE
2 SOON
3 KICK
4 CANOE
5 CAT
6 HURDLE
7 EXACT
8 LATIN
9 GAP
10 MAMMAL
11 LAW
12 INVEST

PIN (optional)

Digital evidence of crypto activity

What is digital evidence of crypto activity?

Digital evidence of crypto activity refers to any content on a traveler's device that suggests ownership, use, or interaction with cryptocurrency. This evidence may not include a wallet itself, but can reveal key leads for further investigation.

Examples of digital evidence include:

- Wallet addresses (copied in emails, chat threads, or notes)
- Transaction hashes and confirmations (e.g. screenshots, PDFs, or email receipts)
- Cryptocurrency QR codes saved as images
- Screenshots of wallet balances, exchange accounts, or mobile app interfaces
- Photos of seed phrases or private keys
- Chat logs or email threads discussing crypto payments, trading, or scams
- Crypto ATM receipts (physical or photographed)
- Login pages or saved credentials for exchanges, DeFi apps, or NFT platforms
- Mentions of tokens or coins in personal messages, spreadsheets, or documents
- Bluetooth connections to hardware or software wallets
- 2FA accounts associated with crypto

Why is it important to identify digital evidence of crypto activity?

Crypto users often leave behind digital footprints that go beyond just financial transactions – they can reveal intent, coordination, and involvement in criminal activity, offering actionable intelligence at the border. These digital traces may help officers determine whether a traveler is a victim of a scam attempting to recover lost assets, an unwitting mule or active facilitator moving illicit crypto across borders, or a suspect engaged in broader networks using cryptocurrency to fund or conceal illegal operations.

Where is digital evidence of crypto activity typically concealed?

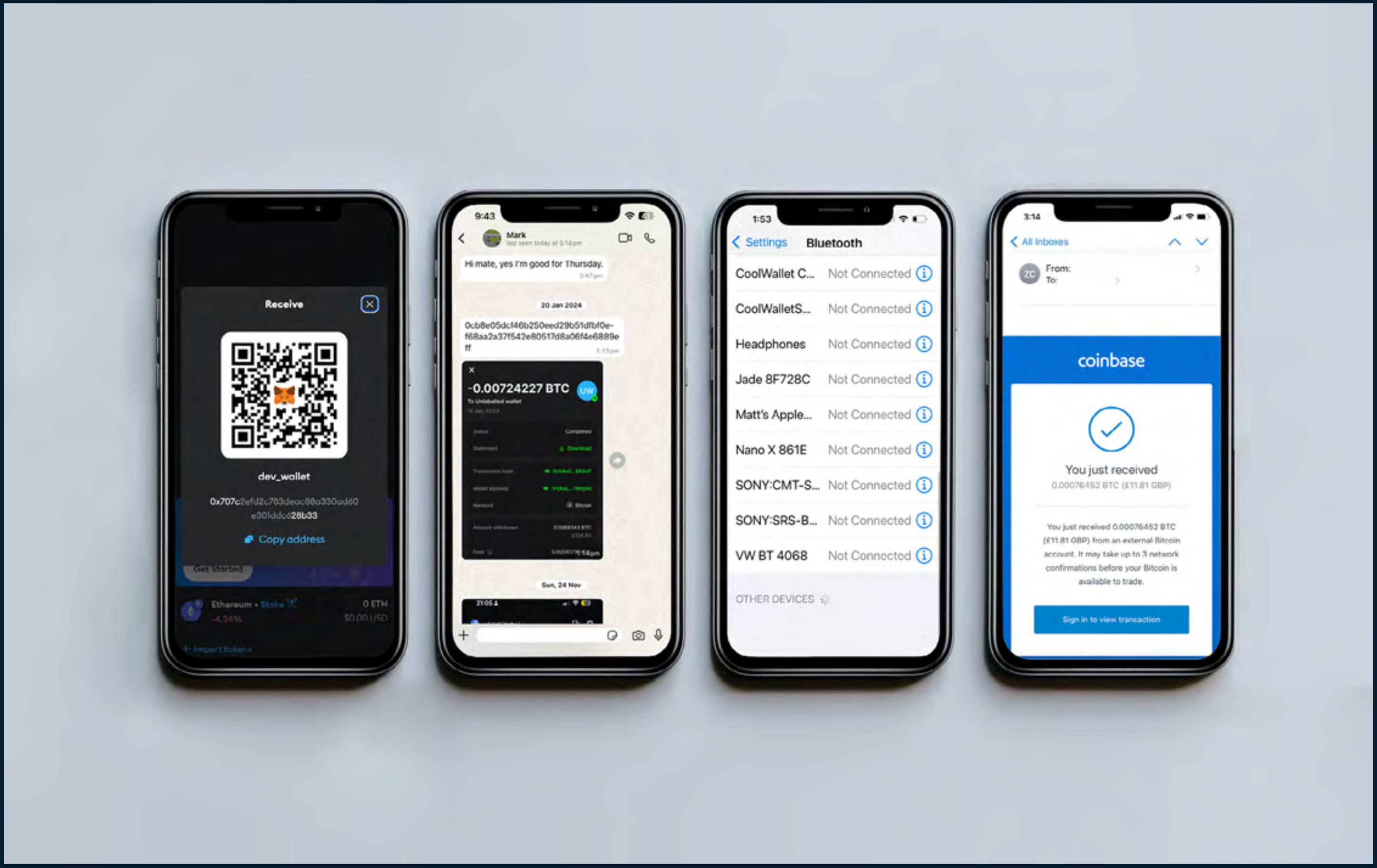
Digital evidence of cryptocurrency activity is often stored on travelers' phones, laptops, or other personal devices. Look for messages, emails, photos, file directories, and chat threads – especially within encrypted apps like Signal, Telegram, or WhatsApp – that may contain screenshots of transactions, wallet addresses, QR codes, or discussions about crypto investments or scams. 2FA apps may also store entries linked to crypto exchanges or wallets, offering additional clues about the traveler's digital footprint.

In addition, the presence of blockchain-specific messaging apps such as Blockscan Chat or Session can indicate a traveler's active interest in blockchain technology. Blockscan Chat requires users to have an Ethereum address to send or receive messages – meaning that if the app is installed, the traveler controls a crypto wallet. Session, while not directly tied to a blockchain wallet, is commonly used by privacy advocates and crypto enthusiasts, and may be a red flag for investigators depending on context.

Digital evidence of crypto activity

Sample questions to ask

- Do you ever chat with anyone about crypto?
- Do you take screenshots or photos, or save images of QR codes, ATM receipts, or crypto addresses?
- Do you get emails from crypto exchanges or other services you use to invest, save, or trade crypto?
- Do you use crypto ATMs? Do you save your ATM receipts?
- Do you use apps like WhatsApp, Kik, Signal, Telegram, or Discord?



Hi mate, yes I'm good for Thursday.

20 Jan 2024

0cb8e05dcf46b250eed29b51dfbf0e-f68aa2a37f542e80517d8a06f4e6889eff

CoolWallet C...	Not Connected
CoolWalletS...	Not Connected
Headphones	Not Connected
Jade 8F728C	Not Connected
Matt's Apple...	Not Connected
Nano X 861E	Not Connected
SONY:CMT-S...	Not Connected
SONY:SRS-B...	Not Connected
VW BT 4068	Not Connected

You just received
0.00076452 BTC (£11.81 GBP)

You just received 0.00076452 BTC (£11.81 GBP) from an external Bitcoin account. It may take up to 3 network confirmations before your Bitcoin is available to trade.

TRM

About TRM Labs

TRM Labs provides blockchain analytics solutions to help law enforcement and national security agencies, financial institutions, and cryptocurrency businesses detect, investigate, and disrupt crypto-related fraud and financial crime. TRM's blockchain intelligence platform includes solutions to trace the source and destination of funds, identify illicit activity, build cases, and construct an operating picture of threats. TRM is trusted by leading agencies and businesses worldwide who rely on TRM to enable a safer, more secure crypto ecosystem. TRM is based in San Francisco, CA, and is hiring across engineering, product, sales, and data science.
To learn more, visit www.trmlabs.com.