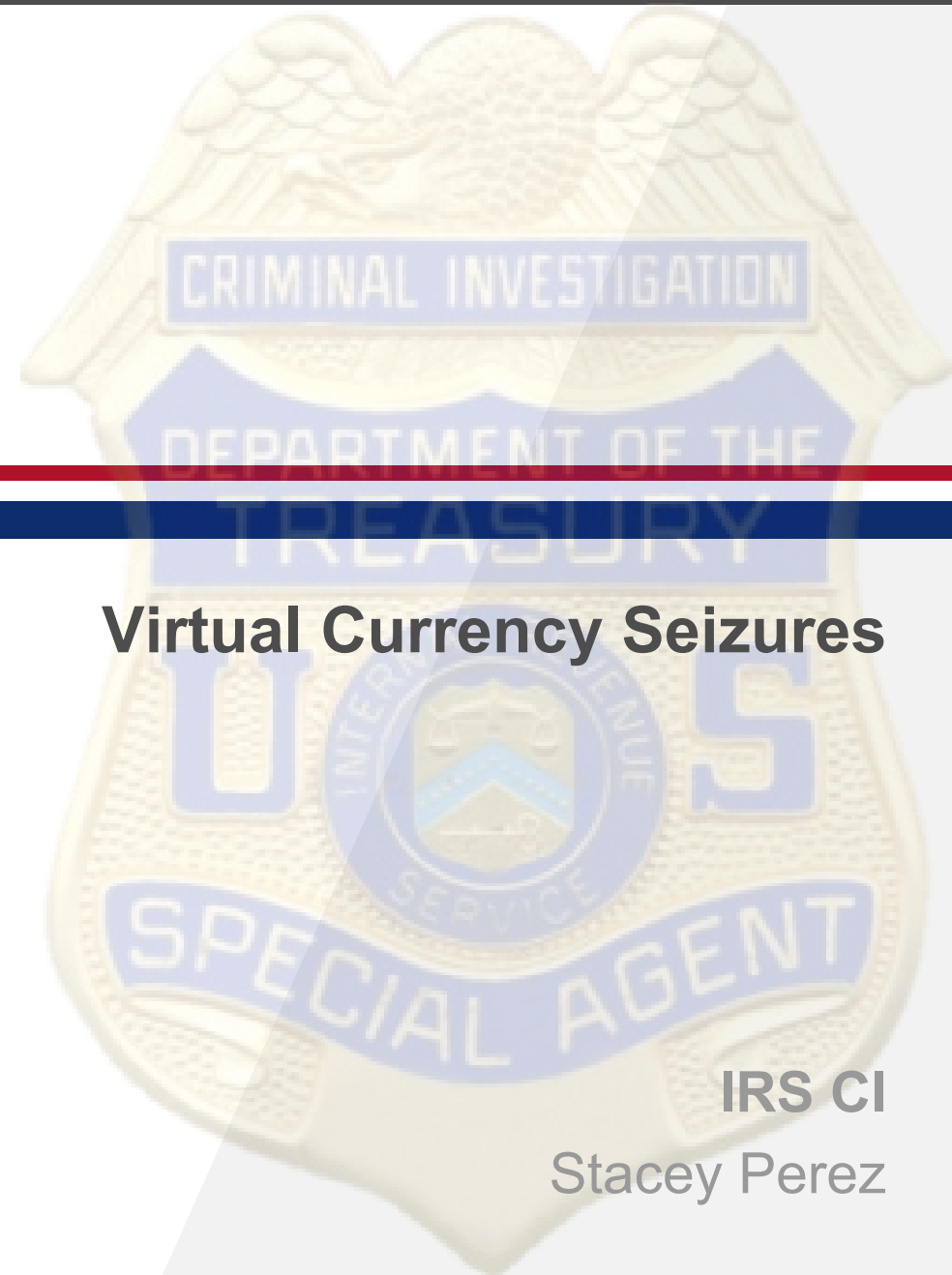




**IRS:CI**

## **Virtual Currency Seizures**



**IRS CI**

Stacey Perez



# Virtual Currency Seizures

FOR IMMEDIATE RELEASE

Monday, November 7, 2022

## **U.S. Attorney Announces Historic \$3.36 Billion Cryptocurrency Seizure And Conviction In Connection With Silk Road Dark Web Fraud**

FOR IMMEDIATE RELEASE

Tuesday, February 8, 2022

## **Two Arrested for Alleged Conspiracy to Launder \$4.5 Billion in Stolen Cryptocurrency**

FOR IMMEDIATE RELEASE

Friday, January 6, 2023

## **Ohio Man Pleads Guilty for Unlawfully Stealing Over 712 Seized Bitcoin Subject to Forfeiture in Brother's Pending Criminal Case**

FOR IMMEDIATE RELEASE

Thursday, February 13, 2020

## **Ohio Resident Charged with Operating Darknet-Based Bitcoin "Mixer," which Laundered Over \$300 Million**



# Agenda

- Seizing Centralized vs Decentralized VC
- Ways to Store VC
- Ways to Seize VC
- Forensics TEAMS
- Seizure Best Practices



# Questions to Ask

What am I seizing?

What Blockchain is it on?



What Kind of wallets do  
Targets Utilize?

Is the crypto Centralized or Decentralized?



# Centralized vs Decentralized

## Decentralized

Bitcoin

Ethereum

## Centralized

USDT (Tether)

XRP

BNB Binance Coin

## Centralized vs. decentralized blockchain

	Centralized	Decentralized
INFORMATION FLOW	To and from center	Multiple routes
DECISION-MAKING	Usually hierarchical	Democratic
CONTROL	Central entity	Software code
PROS	Simpler decision-making, less expensive hardware, more control	Immutability, transparency, member-owned
CONS	Single point of failure, trust issues, data silos	Anonymity for criminals, more expensive hardware, user conflict
EXAMPLES	Binance, Coinbase	Bitcoin, Ethereum





# Storage Matters

coinbase

## Decentralized

Bitcoin ( What if its on an Exchange)

























Ethereum

## Centralized

USDT (Tether)

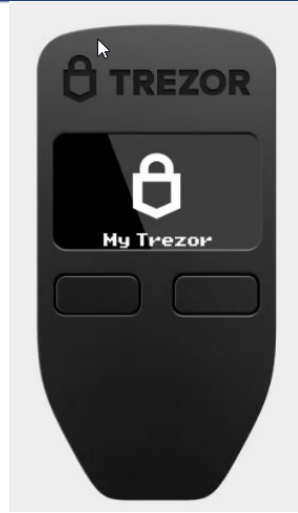
XRP

BNB Binance Coin

























 Exodus	 Electrum	 Coinbase Wallet
 Trezor	 Ledger	 MetaMask
 Coinomi	 Bitcoin Core	 Exodus wallet
 Trezor Model T Advanced...	 Trust Wallet	 Coinbase
 Cryptocurrency wallet ap...	 FAQs	 KeepKey
 Mycelium	 Blockchain.com	 Zengo
 Armory	 BTC wallet	 Guarda
 Edge	 D'CENT Biometric Crypto...	 Atomic Wallet

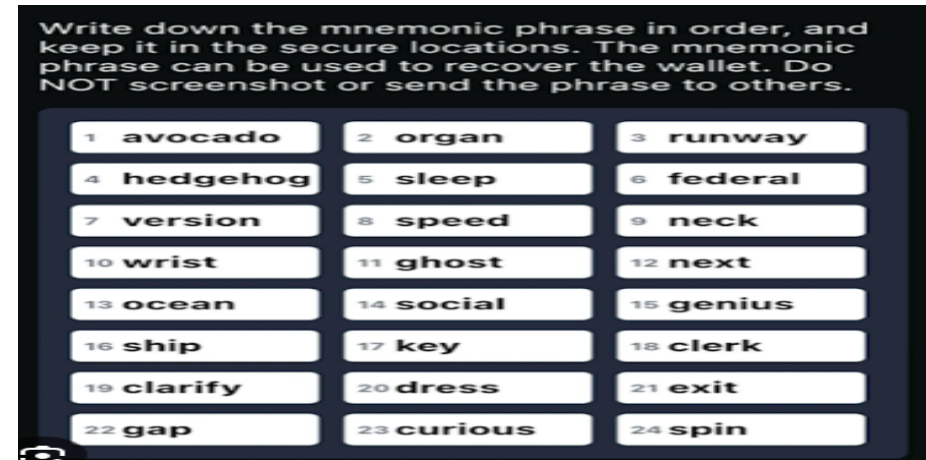


# Storage vs Seed Phrase



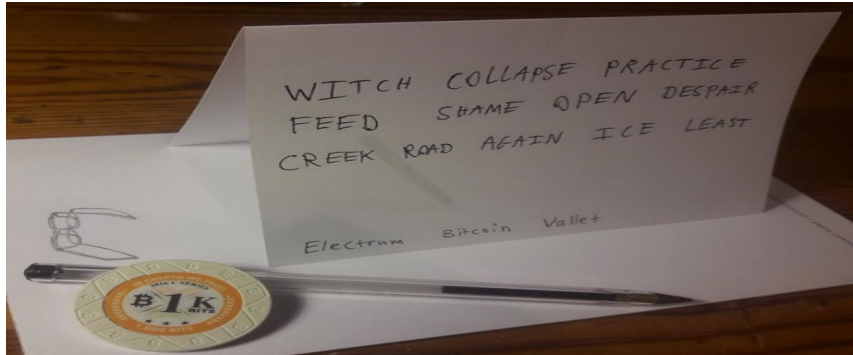
## VS

 Exodus	 Electrum	 Coinbase Wallet
 Trezor	 Ledger	 MetaMask
 Coinomi	 Bitcoin Core	 Exodus wallet
 Trezor Model T Advanced...	 Trust Wallet	 Coinbase
 Cryptocurrency wallet ap...	 FAQs	 KeepKey
 Mycelium	 Blockchain.com	 Zengo
 Armory	 BTC wallet	 Guarda
 Edge	 D'CENT Biometric Crypto...	 Atomic Wallet





# Seizures



A Seed Phrase Only works with the same software that was used to create the wallets



Bitcoin Core



Bitcoin Wallet



breadwallet



Bither



MultiBit HD



Armory



Electrum



mSIGNA



Hive



Mycelium



BitGo



Green Address





# What are Ways to find where VC is being stored





# Purchases



Amazon.com

<https://www.amazon.com/cryptocurrency-hardware-w...>

## Cryptocurrency Hardware Wallet



Model One - The Original Cryptocurrency Hardware Wallet, Bitcoin Security, Store & Manage Over 7000

Coins & Tokens, Easy-to-Use Interface, Quick & Simple Setup ...

30-day returns



Amazon.com

<https://www.amazon.com/Magnetic-GPS-Tracker-Box...>

## Magnetic GPS Tracker Box - Under Vehicle ...

Magnetic GPS Tracker Box - Under Vehicle Waterproof Case, Great Waterproof Hide A Key Strong Magnet Holder (Fits Most Brands, Spytec...

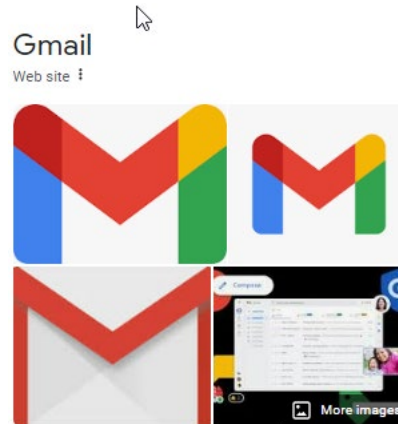
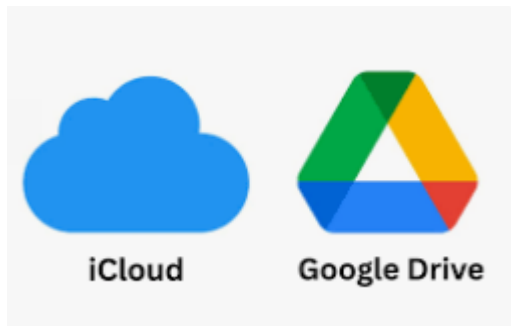
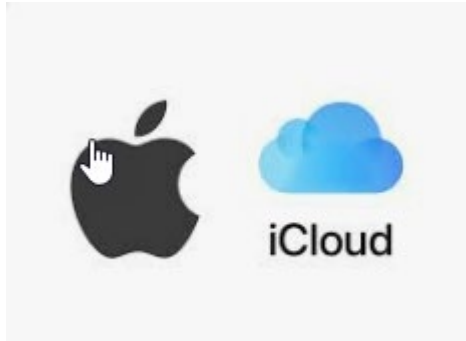
★★★★★ Rating: 4.3 · 15 reviews · \$15.99 · \$5.99 delivery · 30-day returns

· In stock





# Search Warrants





# Search Warrants



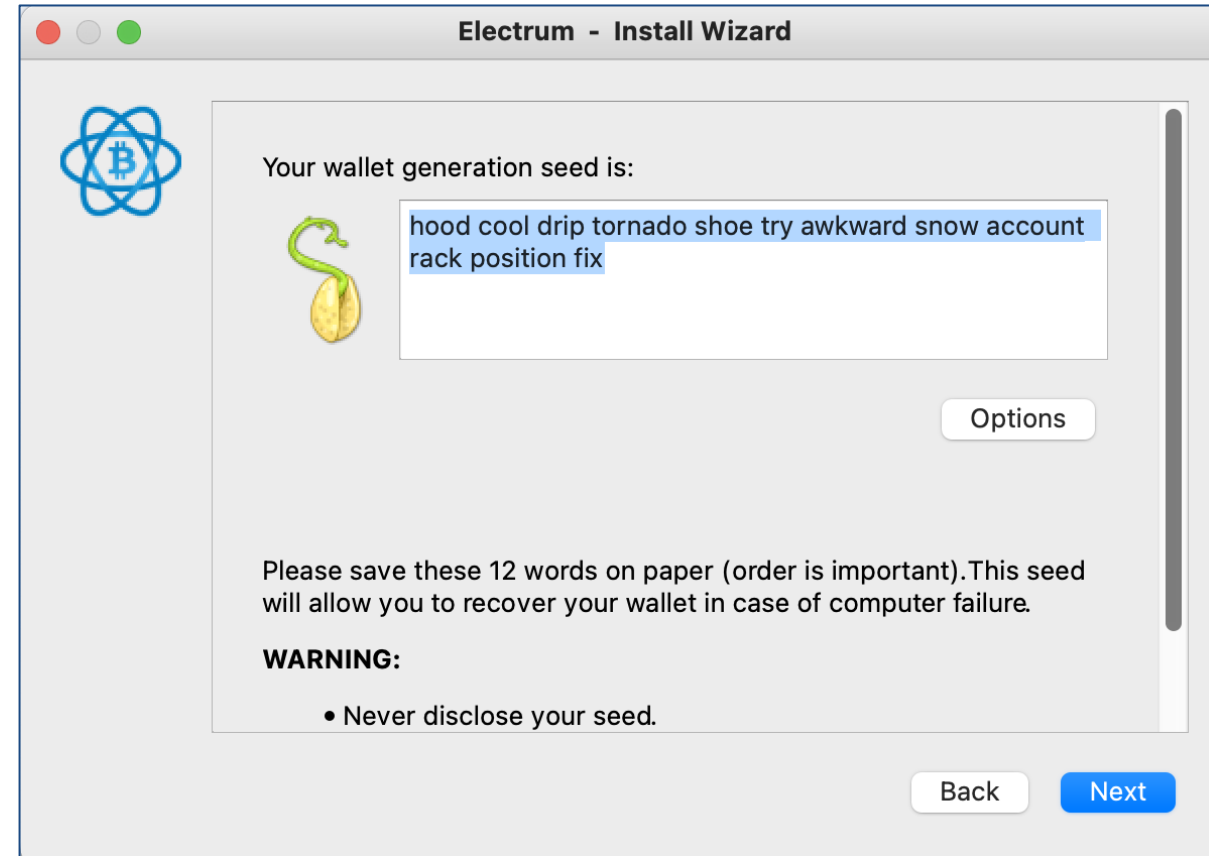




# Forensics TEAM

## Common locations for locating Seed Phrases:

- Screenshots/Photos/Text files stored in:
  - Emails accounts (sent/drafts)
  - Photo apps (Apple Photos, Google Photos)
  - Messaging apps (iMessage, WhatsApp, Signal etc)
  - Desktop/documents folders
  - Cloud storage (Google docs, iCloud)
- Password keepers (LastPass, Keepass etc)







# Wallet analysis and exploitation

The transaction description field frequently contains great evidence (usernames and other notes etc):

Date	Description	Amount
✓ 2013-08-12 23:20	Invoice	+0.32196482
✓ 2013-07-01 15:00	Donation	+0.01
✓ 2013-07-01 14:09	Reddit tipper	+0.01
✓ 2013-06-08 11:31	fund btctip	-0.1501
✓ 2013-06-06 21:48	fund blockchain.info wallet	-0.1001
✓ 2013-06-06 21:08	Fund btctip account	-0.1001
✓ 2013-05-29 01:38	Chargeback	-0.26033527
✓ 2013-05-29 01:04	9flats	-1.32751005
✓ 2013-05-19 20:26	Fund Bitstamp account 3 BTC	-3.0005
✓ 2013-05-16 13:45	NameCheap 25 USD fund account	-0.2196
✓ 2013-05-10 03:05	Bitstamp	+5.99
✓ 2013-01-14 20:32	Reward	+0.52



# Example of text file Containing Private Keys

electrum-private-keys-wallet.csv

address,private_key
bc1qmh5dqq7p3d8rtdhcnkq5l5s0a9j67t3q68nhl,p2wpkh:L3aNpS11GGHuajeR9YDYZ6pnfqcwoZSkhTptKLhqKLcXTnGEokdU
bc1qduuZKhtutdzzwq03y4p0tepvpL7jKmcuXtL0yZ,p2wpkh:L3uR9mimRtKXZivPCZqvVt5tP0pZ93qbyvew4aTpnv3pK0K0A1t9
bc1qdmkqsm625rzda04y58d3ltspu72lm9shqxu45e,p2wpkh:KwxBKW33PYszdvPDKSZU57dKEtHtgxtVJHTujA8wTcHsktP7iKDh
bc1qd9ef2fe4z93smxwz7ltrl9zk5j8xvq0n68ky7s,p2wpkh:L15P4iKM4EUyzBWqTDPEXtAM0i4MAdPa13N9KJqGXpmBqXvGDk5V
bc1qd6c453icfm5nc55cglgn0ux220tjlgpuuayvq,p2wpkh:KyGkayhAgiCmY1dt7cG2Mc2dphB0Xylc20vE+HhucgmYCE2xnn3n

bc1qmh5dqq7p3d8rtdhcnkq5l5s0a9j67t3q68nhl, p2wpkh:L3aNpS11GGHuajeR9YDYZ6pnfqcwoZSkhTptKLhqKLcXTnGEokdU

**Public Key:** bc1qmh5dqq7p3d8rtdhcnkq5l5s0a9j67t3q68nhl

**Script Type:** p2wpkh

**Private Key:** L3aNpS11GGHuajeR9YDYZ6pnfqcwoZSkhTptKLhqKLcXTnGEokdU

bc1qdc70dcexu0y7LqKtLc0Zasume7Cht9tSSy940v5,p2wpkh:KX19vDvaJThyV014157A8GtLC59ScyafEFNqf1J1MPmKvY11e92L

bc1q2y407255zh4zdyuz2ualk5svqa4wtprs8n05uh,p2wpkh:L1qaGB6GDfwTFTA2tqxaMSay1bd9a50vdjL8DXoXTD9cSaYXZphg

bc1q4ul84arwt2cunvf062n5fsj6xrkhgdpkxgjtW3,p2wpkh:L3K5eWxo8SSb4ZeBZZPu6HwoX8kSjZfZqxXC9HtPatjaGp6LS3f1

bc1qk3jincvmsawcu5ipjmfmv24xf4mh2n0nsw3juh,p2wpkh:L3BoFdnrZgeGyxu0fvSUq6D1veMrgH1ZWGoMKzBt0tx7qBZKBGft

bc1qxe6yn3yfkwa55shh6vpwe96uxkyemz2d77rctn,p2wpkh:L3nRRVDPH67U398CPa2d8FrnmLmwDotUErF5baLDnJpWcuSu1Ni

bc1qic2qg4dw42h5veah47hmunf0c5pavc5vvadtrc,p2wpkh:KzbvFAWn4yKYHcZePA15hgHfUWdSgyPw6wPkEPksoWmpvucx1LYL

bc1qhyzian7t82ttfvytegp9mla9v5w0sw3v94yku6,p2wpkh:L3cozsKzzXSvzGB2dwpLwtjVUU4XV5uWzrLHjyncA2NnMGNSSWut

bc1q9h0yju24r8l6qc58087rfsyeffahkael5lh8p0,p2wpkh:L5XgGcbY6ww2nWAdE5L1EaihTr7ni3UGWVS9drGrXq1wDCAtTWww

bc1qjz4qrr6ghpmrqxva7q28dv04dxgn7p0aaf4s7j,p2wpkh:L5bjXGhnRKcfffvoSuj4VsHtwK4vFmEcp2j57nnRC3AXAw0c3W7VF

bc1q40e6k6cucmk3sjxazn8lfjfalnzv6g75gd8nku,p2wpkh:KygcH155XCzXGTiZJU6jKHcNpgXNiwwps6fFKcJ8XNo9cfPJ04TN

bc1qhpeje7qyf7phurz5wi9wlmenmjLmta5d8kxcqu,p2wpkh:L17iJ7CXV2w3zRZBtDCfdG2ecjaKqDtFZrsB6LXejuW1aZM6RzeU

bc1qg3khs6tymdcku7e2anyc7ajlakk5q9rfluf4ms,p2wpkh:KwFe7QYfwDi5EYAKzLEw5xE72ZwnbxxNVm7tF3Km3Vaf5Q1DFDAv

bc1q4gtjl4j286k5pgqkhfcawetynjdha5q8dazfm,p2wpkh:KzS6HanGxnpG90dbHWC8qRpTLanERdfmsEW2fdYEjJficApmhkF

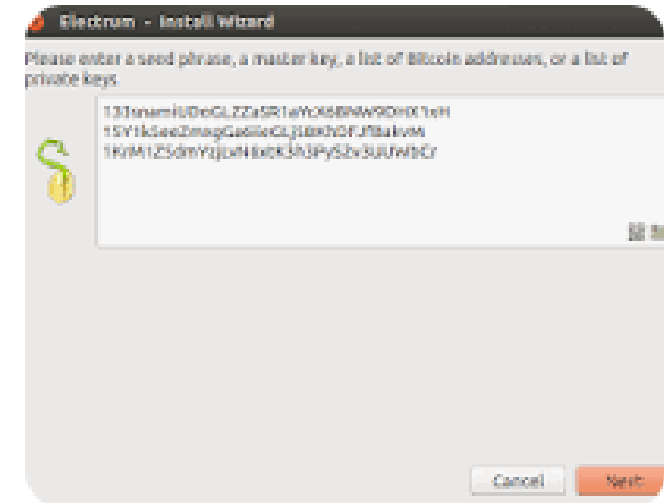
bc1q5jlyaxsysfhn7j5x06vt8n7msquhx9uvff4pl,p2wpkh:Kx0mTtUFYerCrsYKVYUo2toYKjceF64P36je63ipeVV6EePMNmt3

bc1qleefr342fft54wxcjj4sdg8v7pzvu55tttx54j,p2wpkh:KyhxYAgn7YP5wF76mecVnba8R85puwadWMhTifKUmu7idXoA93M3



# Online Research

To restore your wallet from its seed phrase, create a new wallet, select the type, choose “I already have a seed” and proceed to input your seed phrase.



Read the Docs

<https://electrum.readthedocs.io> › latest › faq



Frequently Asked Questions – Electrum 3.3 documentation



# The Truth About Seizures

- Most all virtual currency seizures will require the cooperation of the subject
- Every seizure is different and it is difficult to establish repeatable processes
- Each seizures will likely require working with many of the following:
  - Private Keys
  - Electrum, Metamask, etc ( No KYC WALLETS)
  - Many different smartphone wallet applications , Computers
  - Alt coins ( Gas Fees)

Determining which private keys, seed keys, and master keys go with which wallet (Electrum, Metamask, Bitcoin Core, or other alt coins etc) will require experimentation



# Things to Know

## Working with “keys” notes:

- When restoring a wallet from “keys”, be aware subjects will frequently create “fake” wallet accounts with a small amount of crypto and then hide the real balance in another wallet account
- Depending on the timeframe (i.e. before 2019), don't forget to check historical balances including:
  - Bitcoin Cash (BCH, August 2017) = STOCK SPLIT

## Note

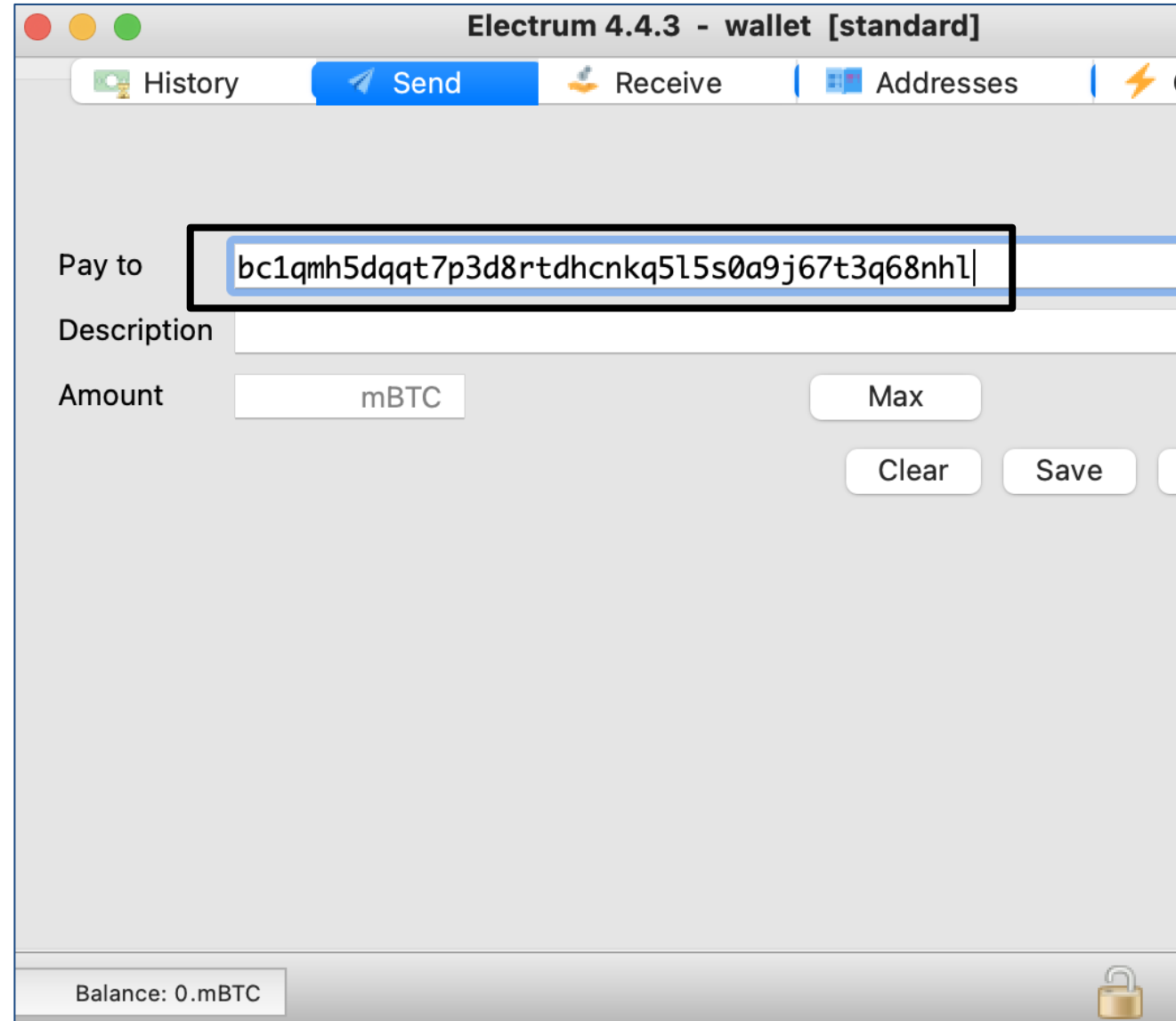
Don't forget to take screenshots or screen video captures of the process for evidentiary and memo purposes.





# Seizure Best Practices

- Copy and paste the **receiving address** to avoid manual transcription issues
- 2 people should independently verify the receiving address
- **Start with a small test transaction (0.01 BTC)**





# Seizure Process

Use the “Max” transaction fee, but verify it is reasonable

Electrum 4.4.3 - wallet [standard]

History Send Receive Addresses Channels

Pay to

Description

Amount  **Max** Clear Save Pay...

Balance: 0.mBTC

**Start with a Test Transaction!!! Enough to Pay fees**



# Do a Test Transaction

- After sending the Test transaction, use a public blockexplorer to monitor the transaction status, (blockchair.com; Blockchain.com; Blockexplorer.com)
- Blocks clear **\*on average\*** every 10 min, but not always in practice
  - Observed many 20 to 40+ minutes blocks during seizures
- One Test Transaction is Confirmed on Blockexplorer and you Check wallet where VC was sent, than conduct the seizure of full amount. (Repeat Steps)

## Transaction

451ee4a3a025524f10e2247b078ac5a62ad524434036ed4154307cd47da1dd32Unconfirmed

First seen	Just now	Fee	17,422 sat <span>\$4.85</span>
ETA	In ~10 minutes	Fee rate	33.5 sat/vB
Features	<span>SegWit</span> <span>Taproot</span> <span>RBF</span>		



# Setup of Wallets

What are things to think about when Transferring the BTC to GOV  
WALLETS?



# Setup of Wallets

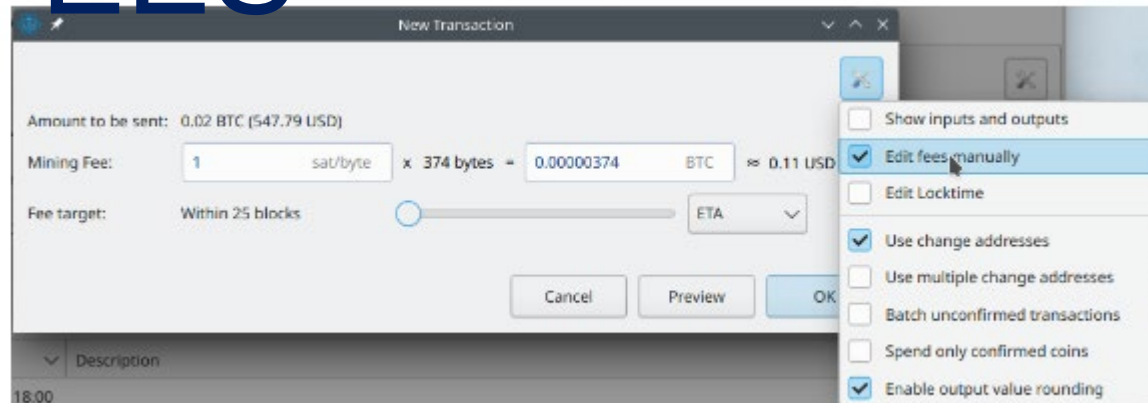
# SCAMS



Wallets with no KYC

- Electrum
- MetaMask
- Wasabi
- Edge

# FEEES



VS

Exchanges





# Seizing Centralized VC

## Circle Confirms Freezing \$100K in USDC at Law Enforcement's Request

Tether welcomes inquiries from law enforcement agencies about its policies and procedures. Please contact Tether at [inforequests@tether.to](mailto:inforequests@tether.to).

In my experience, Circle (USDC), Tether (USDT) and Binance freeze funds for 7 days without a legal order

If you can show probable cause of a crime.

After 7 days have passed, legal order is required.



# Summary

- **Every seizure is different. It requires severe research of target habits, and research into the VC.**
- **Social Media and Purchasing Habits can be crucial to identify how VC is stored**
- **Seizures frequently require assistance from the subject to recover the VC, and a Team**
- **Experimenting yourself with buying Crypto has been vital for me to learn this process**



# Virtual Currency Seizures

