

# Virtual Assets



**Loughnane Associates LLC**  
*Value Touches Everything*

1

## Learning Objectives:

**TLO10. Incorporate an understanding of the various virtual currencies and how they affect financial investigations.**

- |          |  |
|----------|--|
| ELO 10.1 | Define virtual assets.   |
| ELO 10.2 | Identify virtual assets providers and understand their role in an investigation.                 |
| ELO 10.3 | Describe the process flow of virtual assets.   |
| ELO 10.4 | Define intangible property and NFTs and understand their role in financial crime investigations. |
| ELO 10.5 | Understand the differences between the surface, deep, and dark web.                              |
| ELO 10.6 | Describe how an Onion router has a role in financial crime investigations.                       |



2

# Virtual Currency

Training Purposes Only

©2023 Loughnane Associates LLC  
www.loughnaneassociates.com



3

## Convertible Virtual Currency

- A medium of exchange that operated like a currency in some environments
- Does not have legal tender status
- Convertible virtual currency (CVC) has an equivalent value in real currency or acts as a substitute for real currency

*“New types of anonymity-enhanced CVCs have emerged that further reduce the transparency of transactions and identities as well as obscure the source of the CVC through the incorporation of anonymizing features, such as mixing and cryptographic enhancements”*

*“Mixing or tumbling involves the use of mechanisms to break the connection between an address sending CVC and the addresses receiving CVC. “*



FinCEN. (2019, May). Advisory on Illicit Activity Involving Convertible Virtual Currency. <https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf>

Training Purposes Only

©2023 Loughnane Associates LLC  
www.loughnaneassociates.com



4

# Virtual Asset Service Providers

Training Purposes Only

©2023 Loughnane Associates LLC  
www.loughnaneassociates.com



5

## “Virtual Assets” And “Virtual Asset Service Providers”



Department of the Treasury  
Financial Crimes Enforcement Network

Guidance

FIN-2013-G001

Issued: March 18, 2013

Subject: Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies



FinCEN ADVISORY

FIN-2019-A003

May 9, 2019

Advisory on Illicit Activity Involving Convertible  
Virtual Currency

*Criminals continue to exploit virtual currency to support illegal activity, money laundering, and other behavior endangering U.S. national security, including through entities facilitating its anonymous use.*



Training Purposes Only

©2023 Loughnane Associates LLC  
www.loughnaneassociates.com



6

## Common KYC Requirements

- Full name
- Date of birth
- Phone number and/or email address
- Physical address and/or country of residence
- Photo/scan of government-issued ID such as a driver's license or passport
- Copy of utility bill
- Photo of yourself with your ID

Training Purposes Only

©2023 Loughnane Associates LLC  
www.loughnaneassociates.com



7

## Virtual Asset Service Providers

- Classified as Money Services Businesses
  - Remember the requirement for foreign registration
- FATF defines Virtual Asset Service Provider (VASP) as:
  - Any natural or legal person who is not covered elsewhere under the FATF Recommendations
  - As a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:
    - exchange between virtual assets and fiat currencies;
    - exchange between one or more forms of virtual assets;
    - transfer of virtual assets;
    - safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
    - participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.



Training Purposes Only

©2023 Loughnane Associates LLC  
www.loughnaneassociates.com



8

# Travel Rule

All financial institutions are required to pass on certain information to the next financial institution, in certain funds transmittals involving more than one financial institution

## Transmitter Side:

- ✓ Name, Address
- ✓ Account number if used
- ✓ Identity of Financial Institution
- ✓ Amount transmitted
- ✓ Execution date
- ✓ Identity of Recipient's Financial Institution

## Recipient Side:

- ✓ Name, Address
- ✓ Account number
- ✓ Any other specific identifier

## Intermediary Bank:

- ✓ Required to pass on all information from Transmitter Bank
- ✓ Or proceeding Intermediary

**Exception - If Transmitter and Recipient are the same Financial Institution**

Training Purposes Only

©2023 Loughnane Associates LLC  
www.loughnaneassociates.com



9



Access to Perfect Money accounts from the United States is not allowed.

Services of Perfect Money are not available to US citizens or US residents. This includes US residents/citizens leaving overseas. In short, if you live in the USA,

- In operation since 2007
- Says it is based in Panama, but the Panamanian government says no
- Once a user obtains an account, they can transfer Perfect Money units to other users inside the system
- Southern Methodist University 2011 study – Liberty Reserve and Perfect Money were two of the most widely accepted digital currencies for online Ponzi schemes
- Of 1,000 websites that linked to Perfect Money, they found 70% that were Ponzi schemes

**All Account that belong to US Citizens/Residents/US Companies will be disabled within 15 days  
15.06.13**

Dear Customers,

In line with our policy, all accounts that belong to US Citizens/Residents/US Companies will be disabled on 1st of July. If you still have funds on your account, please take appropriate and timely steps to withdraw the balance. Please note that after 1st of July, no transactions can be executed at accounts that fall into the above mentioned category.

Please do not postpone taking action to withdraw you balance.

Training Purposes Only

©2023 Loughnane Associates LLC  
www.loughnaneassociates.com



10

# The Process



## Let's Work With Bitcoin

### What is Bitcoin?

- An electronic payment system based on mathematical proof
- Decentralized
- Low transaction fees?
- Built on a "Blockchain" technology which ties to a PKI infrastructure
  - Public Key
  - Private Key
  - Proof - of - Work
- Owner is determined by the last transaction

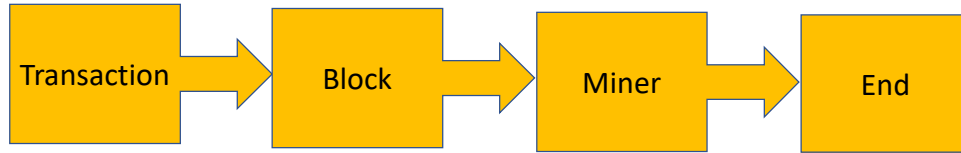
### How Does a Transaction Work?

- Requires a Bitcoin wallet, a Bitcoin, and a wallet address
- Transaction is placed in a Transaction Block
- Authenticated by "Bitcoin Miners" who get paid in Bitcoin as they authenticate a transaction
- Transfer is verified and distributed to public ledgers

Who is  
Satoshi Nakamoto?



# Process Flow



Mark wants to send 1 BTC to Jessica. He uses his private key to 'sign' a message with the transaction-specific details.

.6 BTC + .6 BTC to Jessica  
(.2 BTC returned to Mark)

Mark's transaction is placed in a Transaction Block with other transactions.

This Block is ciphered and then is attacked by Bitcoin Miners.

Whichever Miner breaks it first gets to authenticate the transactions

Miners authenticate transaction in blocked and are paid for the process

About 10 minutes after transaction approval is given and it completes

Training Purposes Only

©2023 Loughnane Associates LLC  
www.loughnaneassociates.com



13

Blockchain.com | Wallet | Exchange | Explorer | Buy Bitcoin | Trade

Explorer > Bitcoin Explorer > Block

Search your transaction, an address or a block

**Block 680045**

This block was mined on April 21, 2021 at 2:57 PM EDT by [BTC.TOP](#). It currently has 1 confirmations on the Bitcoin blockchain.

The miner(s) of this block earned a total reward of 6.25000000 BTC (\$346,854.88). The reward consisted of a base reward of 6.25000000 BTC (\$346,854.88) with an additional 3.18375474 BTC (\$176,688.14) reward paid as fees of the 3162 transactions which were included in the block. The Block rewards, also known as the Coinbase reward, were sent to this [address](#).

A total of 62,295.57728239 BTC (\$1,572,033,947.41) were sent in the block with the average transaction being 19.70132109 BTC (\$1,093,359.88). Learn more about [how blocks work](#).

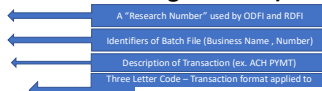
Hash	000000000000000000000008ef389946235866b69b2b7a1859b8e1b540e0702a629b
Confirmations	1
Timestamp	2021-04-21 14:57
Height	680045
Miner	<a href="#">BTC.TOP</a>
Number of Transactions	3162

14

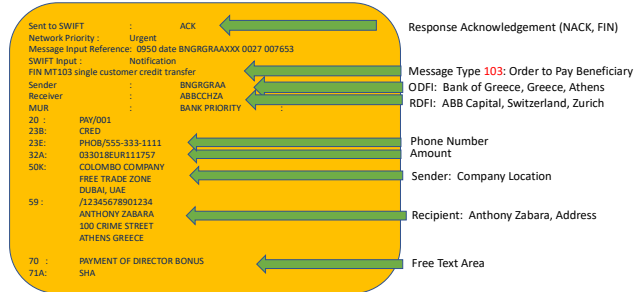
# Pseudo-Anonymous

## ACH Data (formatted to NACHA guidelines)

- Trace Number
- Batch Name/Number
- Company Entry Description
- Standard Class Entry Code
- ODFI/RDFI Identification Number
- ODFI/RDFI Account Numbers
- Type of Transaction/Transaction Code
- Recipient Name/Identification Number
- Recipient Account Number
- Sender Name
- Sender RDFI Account Number



## SWIFT Message Data



www.valuetoucheseverything.com

Training Purposes Only

www.valuetoucheseverything.com

Training Purposes Only

©2021 Loughnane Associates LLC



Training Purposes Only

©2023 Loughnane Associates LLC

www.loughnaneassociates.com



15

# Pseudo-Anonymous

Blockchain.com
Buy Bitcoin Trade

### Summary

This transaction was first broadcast to the Bitcoin network on April 21, 2021 at 8:10 AM EDT. The transaction currently has 2 confirmations on the network. At the time of this transaction, 0.28324024 BTC was sent with a value of \$15,526.79. The current value of this transaction is now \$15,718.92. [Learn more about how transactions work.](#)

Hash	Amount	Date
043000d5fd9602ad5adbee3b063d047b1384dc7189deba835...		2021-04-21 08:10
1MUvgqe48G33qo1guHHz3ypD3udLnRUeRA4	0.12350422 BTC	➔
1pVGyX1U9JgeERdsiTo6zdmQQzR55eHT9	0.16020304 BTC	
	1MCrzd7TVSxmrqF4tkGo2CBYDYWgyoxKthj	0.01506969 BTC
	3MrWkEkWJ75hqZ8ti6m6WWGqz1yTFA6Ws	0.00110000 BTC
	18Xg5cPz9WN8g4icqqjW3dLBrgrbPTPqk	0.00349123 BTC
	1KIXfP3xiYBVpzArj2HSEPCiQFtsodc26	0.02980000 BTC
	1JQsqQnASTf9dkRzYDiwNscJ7NidELKGC	0.01355008 BTC
	bc1q5kegwgrp55zuqpt0d98jgkhrtdwnzdxk...	0.00087608 BTC
	1LxsfZznPvFpznDNUdov6BsgdYQ4A6VhYj	0.19951096 BTC
	1NUw12vXddMf6tYTG1oR2R9yY2r98ypSWC	0.01984220 BTC

Fee: 0.00046702 BTC (81.790 sat/B - 20.447 sat/WU - 571 bytes)

0.28324024 BTC  
2 Confirmations

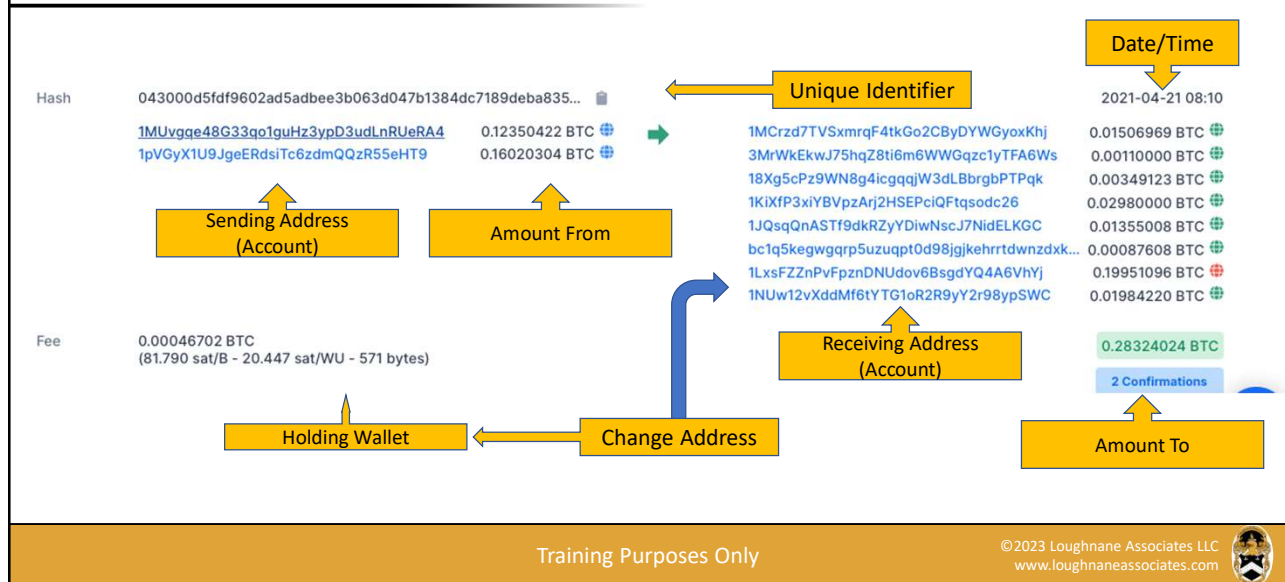
Training Purposes Only

©2023 Loughnane Associates LLC  
www.loughnaneassociates.com

16

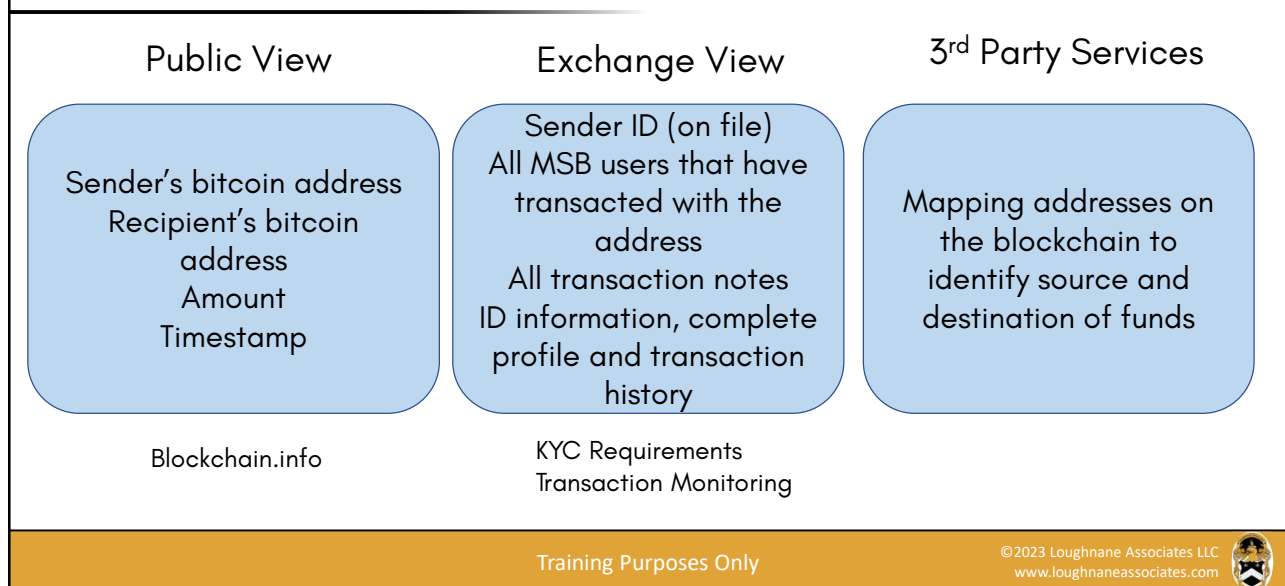


# The Information is Here (Blockchain.info)



17

# Transaction Views



18

## Public View



Blockchain.com Wallet Exchange Explorer Buy Bitcoin Trade

Sponsored Content

Explorer > Bitcoin Explorer

15K9Z1AU2hT3ebZMtWqDsMv3fTxTNwpf USD

### Bitcoin

Blockchain information for Bitcoin (BTC) including historical prices, the most recently mined blocks, the mempool size of unconfirmed transactions, and data for the latest transactions.

\$55,496.78 Price →	127,777 EH/s Estimated Hash Rate →	242,727 Transactions (24hrs) →	1.949m BTC Transaction Volume →	127,892 BTC Transaction Volume (Est) →
------------------------	---------------------------------------	-----------------------------------	------------------------------------	---

Price 1 Day ↓ Mempool Size (Bytes) 1 Day ↓

Training Purposes Only

©2023 Loughnane Associates LLC  
www.loughnaneassociates.com



19

## Method To Identify/Track A Bitcoin Address Owner

- Personal Information Posted: Collecting donations on a personal blog
- Posting an address on a website using their real name as owner of registered domain
- Use real identity in a forum with address
- Use of address in social media (Facebook, LinkedIn, etc.)
- Tracking Outside Purchases (name and shipping information?)
- Searching for Thin Client or Hosted Wallet Usage
- IP transactions traced by the Internet Service Provider
- Identify the exchange holding the account who logs transactions
- Using Transaction Analysis software firms such as Elliptic or Chainalysis

Training Purposes Only

©2023 Loughnane Associates LLC  
www.loughnaneassociates.com



20

# Blockchain Analysis: Suspect Addresses



QR code for address: 15K9Zj1AU2hjT3ebZMtWqDsMv3fXtNwpf

Address	15K9Zj1AU2hjT3ebZMtWqDsMv3fXtNwpf #
Format	BASE58 (P2PKH)
Transactions	23
Total Received	0.00036343 BTC
Total Sent	0.08945595 BTC
Final Balance	0.00090748 BTC

Transactions

Hash	Amount	Time
7adcf6a160e556042b88c1f1d8b04847ecd5c145af3b631... 16w8GWBW7J5BvgPZqKka2GaJL8...	0.00096279 BTC	2020-11-05 08:31
15K9Zj1AU2hjT3ebZMtWqDsMv3fXt... 1C87H84PyMM3Bndy9Dw2ATEk...	0.00022857 BTC	
Fee	0.00006300 BTC	
Hash	0.0011557 BTC	2020-11-05 08:05
1M6qucd5brqhs544zUe1TRWsaNv... 1M6qucd5brqhs544zUe1TRWsaNv...	0.00109000 BTC	
15K9Zj1AU2hjT3ebZMtWqDsMv3fXt... 16w8GWBW7J5BvgPZqKka2GaJL8...	0.00098279 BTC	
Fee	0.00004200 BTC	
Hash	0.00010000 BTC	2020-10-28 01:59
19aakUo6c8dzxwBzh0BWWjYyKwN... 113L8c4a9228Kx6w0ALUWhUdzpfs...	0.00011816 BTC	

Money going to...  
Money coming from...

Identify other suspect addresses



# Blockchain Analysis: Clustering

Association with suspect addresses


Pull history of the use of these addresses

1MCrzd7TVSxmrqF4tkGo2CByDYWGyoxKhj  
3MrWkEkWJ75hqZ8ti6m6WWGqzc1yTFA6W5  
18Xg5cPz9WN8g4icgqjW3dLBbrgbPTPqk  
1KiXfP3xiYBVpzArj2HSEPCiQFtqsodc26  
1JQsqQnASTf9dkRZyYDiwNscJ7NidELKGC  
bc1q5kegwqrp5uzuqpt0d98jgkhehrrtdwnzdxk..  
1LxsFZZnPvFpznDNUdov6BsgdYQ4A6VhYj  
1NUw12vXddMf6tYTG1oR2R9yY2r98ypSWC



**Address** USD BTC

This address has transacted 402 times on the Bitcoin blockchain. It has received a total of 767.11468021 BTC (\$29,102,044.97) and has sent a total of 767.11468021 BTC (\$29,102,044.97). The current value of this address is 0.00000000 BTC (\$0.00)



Address	1AVKdnyWRQJbqS4H3GrvG5fapdTapBnW9u
Format	BASE58 (P2PKH)
Transactions	402
Total Received	767.11468021 BTC
Total Sent	767.11468021 BTC
Final Balance	0.00000000 BTC

**Transactions**

Hash	19d0e4c4f79f3d907e05fa2654e571ab9767b8efc968ba33e0c3	2021-03-15 11:20
	...1AVKdnyWRQJbqS4H3GrvG5fapdTapBnW9u 2.272727 BTC	→ 1QEojScgoRXJfwMidWFeVLWCQoo6BFUXg 0.08899316 BTC
Fee	0.00026502 BTC (81.046 sat/B - 20.261 sat/WU - 327 bytes)	-114116106 BTC
		5 Confirmations
Hash	e6c4eab972d73686448f684a7c07080afec20fc7b489c7af2f1	2021-03-24 09:40
	1AVKdnyWRQJbqS4H3GrvG5fapdTapBnW9u 1.4343443 BTC	→ 1QEojScgoRXJfwMidWFeVLWCQoo6BFUXg
Fee	0.00023755 BTC (81.075 sat/B - 20.269 sat/WU - 293 bytes)	+114116106 BTC

Training Purposes Only ©2023 Loughnane Associates LLC [www.loughnaneassociates.com](http://www.loughnaneassociates.com)

23

## Crypto Money Laundering Scenario

MSB TMS alerts to large bitcoin deposit for account holder

➔

Source addresses identified and assessed

➔

Several source addresses associated to dark web site selling narcotics

➔

Suspect addresses show multiple addresses for money in, two for money out (account holder is one)

Track account holder money out to 2 accounts in another exchange – No other deposits identified

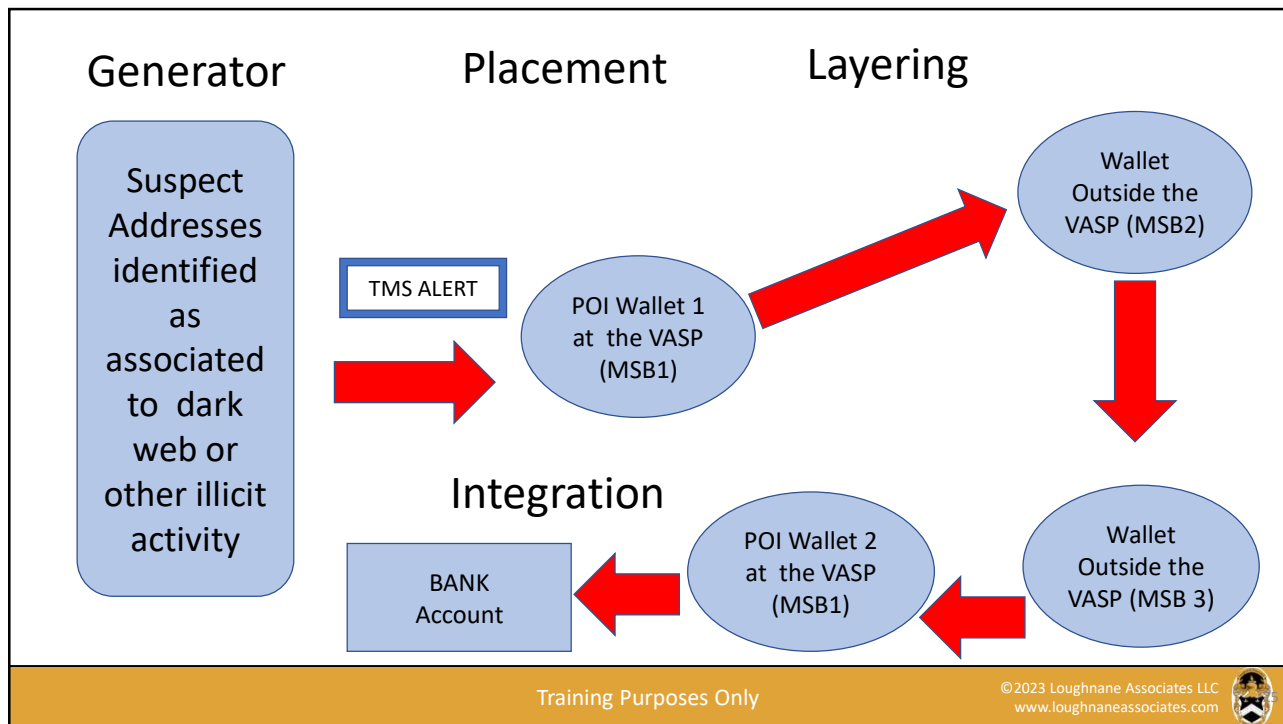
➔

Money out from external accounts come back to another account in exchange

What can we deduce?

Training Purposes Only ©2023 Loughnane Associates LLC [www.loughnaneassociates.com](http://www.loughnaneassociates.com)

24



25

## Consider Third Party Options

- Fast way to identify suspect clusters
- There are analyst providers who have prepared the attribution to addresses and have them clustered
- OSINT third party providers such as:
  - Blue Lights Digital Training
  - Flashpoint
  - Others

©2023 Loughnane Associates LLC  
www.loughnaneassociates.com

26

## Chain of Custody

- Know your organization's policies
- There needs to be complete audit trails
- Chain of custody and accountability for activity is critical
- Consult & team with experts, especially if you are building a case
  - You need the tools
  - You need the testimony

Training Purposes Only

©2023 Loughnane Associates LLC  
www.loughnaneassociates.com



27

## Don't Forget The "Old School" Financial Investigation Methods

- How does the suspect purchase equipment and material related to the crime?
- Shipments are paid? - Cash? Credit Card? Debit Card? Prepaid Access?
- Track the credit card transactions
- Track the prepaid access cards
  - How is suspect loading them? At the counter at Walmart? What is suspect doing to load them?
- Is the Exchange account associated to a bank account?
  - Do the bank records show transfers/receipts from a VASP?
  - Where does the cryptocurrency convert to fiat? And what happens to the money?
- Subpoenas, Warrants, Seizures, Interviews, Informants, Cellphone and Surveillance, and so much more

Training Purposes Only

©2023 Loughnane Associates LLC  
www.loughnaneassociates.com



28

Pocket Litter!

Element peach process pyrrhic...

Keep it!



## Privacy Coins

What they are:

- Cryptocurrencies that power private and anonymous blockchain transactions
- They obscure their origin and destination.
  - Impossible to determine who owns how many coins, or who is sending and receiving transactions.
  - Only transaction participants (senders, recipients, or those with certain "view" keys) can view transaction data.
  - Mixing multiple transactions with each other to elude chain analysis.
- While privacy coins are not banned yet, they are making things difficult for both countries and exchanges that are subject to information-sharing requirements due to regulations like the FATF Travel Rule.
  - Many exchanges have delisted



Dash



Monero



Zcash



Beam



Grin



# Privacy Coins



Dash



Monero



Zcash



Beam



Grin

## How they work:

- Stealth addresses require a sender to generate a new address for every transaction sent in order to avoid being linked to a receiver.
  - Monero uses a version called the dual-key stealth address protocol (DKSAP).
- CoinJoin: A coin mixer that merges transactions from various individuals into a single transaction and then disburses them to their respective users using new addresses.
- Zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) allow cryptocurrency holders to prove a transaction's validity without divulging critical identifying information such as the parties involved and the account balances.

The challenge is how these coins will align with FATF compliance requirements

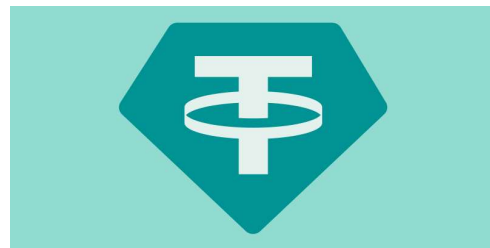
Chainalysis and CipherTrace both say they have tools to trace Privacy Coins



# Stable Coins

## What they are:

- True to their name, stablecoins are intended to provide the stability ordinarily found in traditional assets within the otherwise volatile crypto market because of their supposed 1-to-1 match to a FIAT currency.
  - Tether (USDT)
  - USD Coin (USDC)
  - TrueUSD (TUSD)
  - Paxos Standard (PAX)
  - Gemini Dollar (GUSD)
  - MakerDAO Stablecoin (DAI)
  - STASIS EURS (EURS)
  - Singapore Dollar Rate (SGDR)





# CBDC - Central bank digital currency

What they are:

- A CBDC is a central bank digital currency. They are digital versions of a nation-state currency issued by the central bank of a given nation. They may or may not be backed by another asset or they may exist purely as fiat currency, which means the value is based on the promise of the government. Most major nation-states use fiat currency today and you could think of CBDCs as a digital version of fiat that has special unique additions in capabilities and functions because it's purely digital.
- For example, in the US, a CBDC would essentially be a "digital dollar" and is often referred to as such.



Sources: Pixabay, Facebook ECCB Connects.

Training Purposes Only

©2023 Loughnane Associates LLC  
www.loughnaneassociates.com



33

# CBDC - Central bank digital currency

- Studies of how to apply CBDCs and begin issuing them are underway from several major nations across the globe. Some countries have already successfully launched their CBDCs, including Nigeria .
- The important thing you need to know is that CBDCs are different from Bitcoin and other cryptocurrencies because they are created and governed by a centralized authority—in this case, a nation-state. You can make the case that many cryptocurrencies are also centralized, but there are many that fall on the spectrum of decentralization, and this is what makes them unique from our current legacy financial system.



Sources: Pixabay, Facebook ECCB Connects.

Training Purposes Only

©2023 Loughnane Associates LLC  
www.loughnaneassociates.com



34

# Non-Fungible Tokens

- NFTs are unique cryptographic tokens that exist on a blockchain and cannot be replicated.
- NFTs can be used to represent real-world items like artwork and real-estate.
- "Tokenizing" these real-world tangible assets allows them to be bought, sold, and traded more efficiently while reducing the probability of fraud.
- NFTs can also be used to represent peoples' identities, property rights, and more.



Training Purposes Only

©2023 Loughnane Associates LLC  
www.loughnaneassociates.com



35

Larva Labs      Projects    Writing    About

CryptoPunks Overview

### Punks for Sale

Transaction History

Cryptopunks / 3621

### CryptoPunk 3621

One of 3840 Female punks.

**Accessories**

**Mohawk** 441 punks have this.      **Earring** 2459 punks have this.      **Cigarette** 961 punks have this.

**Current Market Status**

This punk is currently owned by address **0xf4a775**.  
This punk is currently for sale by owner for 20E (\$38,123).  
There are currently no bids on this punk.

**Transaction History**

Type	From	To	Amount	Txn
Offered			20E (\$33,764)	Mar 28, 2021
Offer Withdrawn				Mar 12, 2021
Offered			25E (\$44,471)	Mar 11, 2021
Offered			20E (\$36,995)	Mar 10, 2021
Sold	0xb6be4d	0xf4a775	0.09E (\$42)	Dec 03, 2017
Offered			0.09E (\$26)	Nov 01, 2017
Claimed		0xb6be4d		Jun 23, 2017

Training Purposes Only

©2023 Loughnane Associates LLC  
www.loughnaneassociates.com



36

Questions?

**Loughnane Associates LLC**  
*Value Touches Everything*

