



**ISACA.**  
CONFERENCE  
Europe 2021  
HYBRID EVENT

# OSINT Methods and Techniques for Blockchain Investigators and IT Auditors

Tuan Phan, CISSP, PMP, CTCE, CBSP, SSBB

Zero Friction LLC

[tphan@zerofriction.io](mailto:tphan@zerofriction.io)

Please include the  
**HOUSEKEEPING REMINDERS** slide  
at the beginning of your presentation and the  
**THANK YOU** slide  
at the end.

Any questions, please let us know. Thank you!

# HOUSEKEEPING REMINDERS

- Take a moment to clear your things from the unoccupied seats near you to allow others to sit.
- Please always wear your name badge; it is your ticket into all conference events.
- Be sure to complete the session evaluation on the mobile app at the end of each session!
- If slides or handouts are available, they can be downloaded from the mobile app or conference website.
- Please make sure your cell phone is turned to silent during every session.

# Thank you!

Don't forget to fill out the session survey located within the mobile app after this and every session!

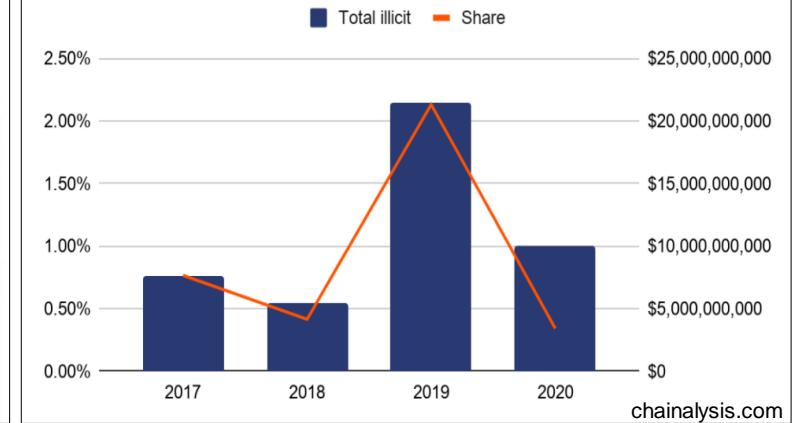
# Why do we conduct blockchain investigations?

Meat giant JBS pays \$11m in ransom to resolve cyber-attack

10 June



Total cryptocurrency value sent and received by criminal entities vs. Criminal share of all cryptocurrency activity,



chainalysis.com



Photographer: Samuel Corum/Bloomberg

Cybersecurity

## Hackers Breached Colonial Pipeline Using Compromised Password

By William Turton and Kartikay Mehrotra

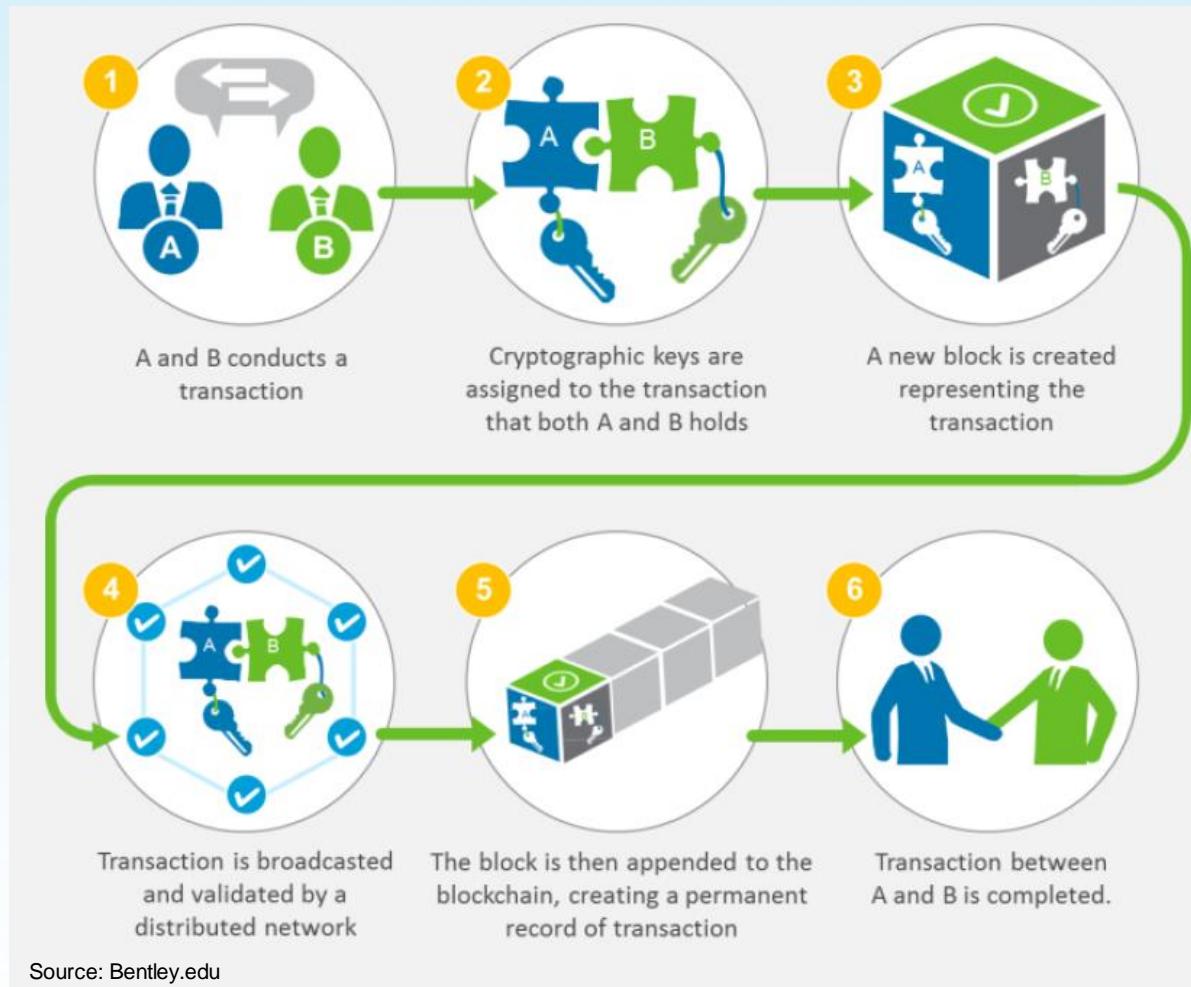
June 4, 2021, 3:58 PM EDT

- ▶ Investigators suspect hackers got password from dark web leak
- ▶ Colonial CEO hopes U.S. goes after criminal hackers abroad



# How Blockchain Works?

## Quick Recap



Source: Bentley.edu

# Distributed Network & Shared Ledger

## GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Mon Jul 26 2021 06:49:20 GMT-0400 (Eastern Daylight Time).

### 12307 NODES

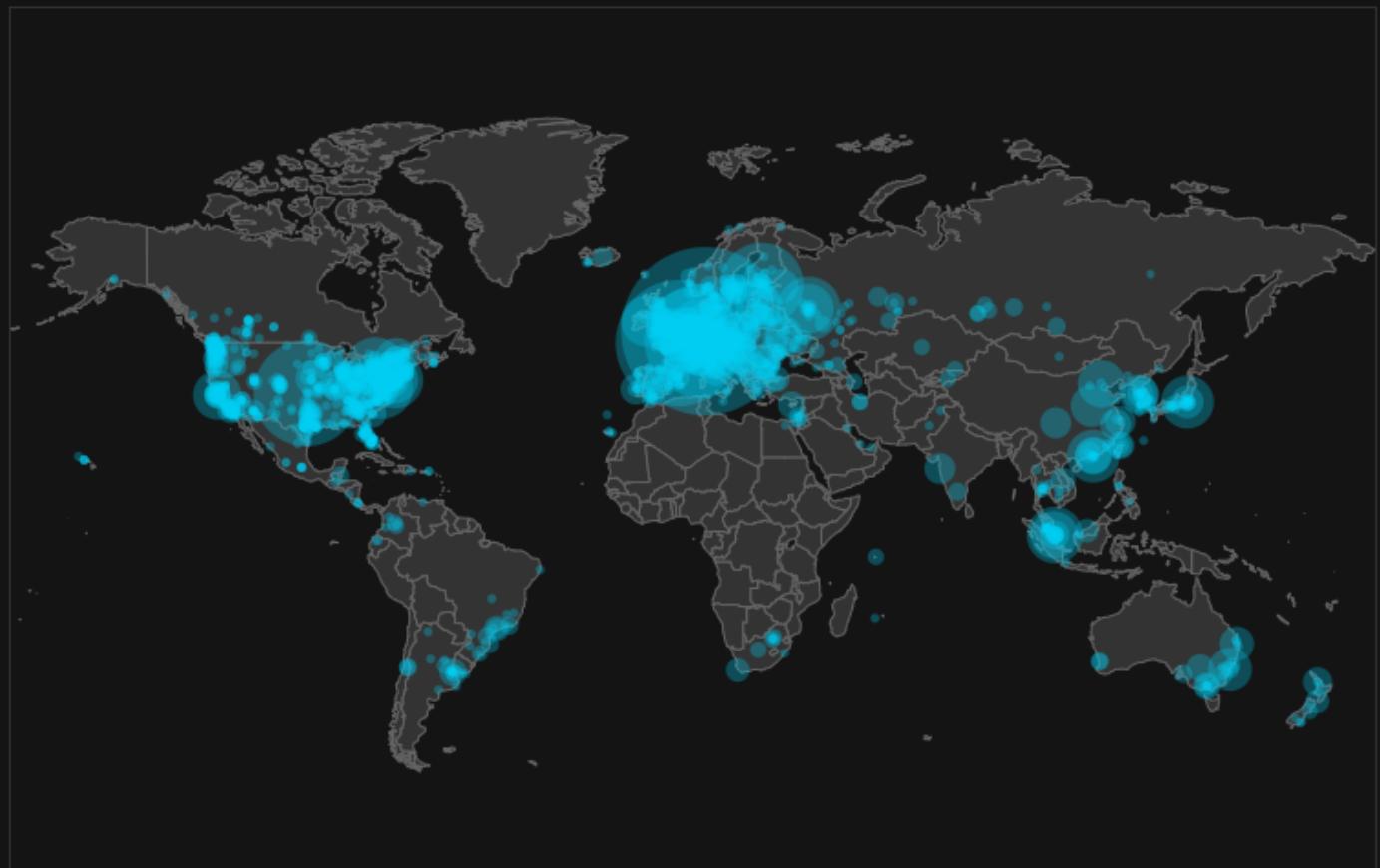
[24-hour charts »](#)

Top 10 countries with their respective number of reachable nodes are as follow.

| RANK | COUNTRY            | NODES         |
|------|--------------------|---------------|
| 1    | n/a                | 5014 (40.74%) |
| 2    | United States      | 1792 (14.56%) |
| 3    | Germany            | 1673 (13.59%) |
| 4    | France             | 539 (4.38%)   |
| 5    | Netherlands        | 405 (3.29%)   |
| 6    | Canada             | 306 (2.49%)   |
| 7    | United Kingdom     | 250 (2.03%)   |
| 8    | Russian Federation | 214 (1.74%)   |
| 9    | Finland            | 185 (1.50%)   |
| 10   | Switzerland        | 152 (1.24%)   |

Source: [bitnodes.io](#)

[More \(91\) »](#)



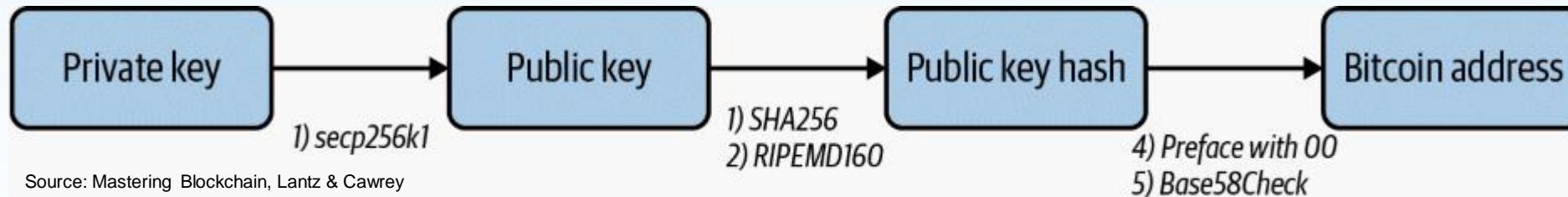
# Identity Management of *Typical* Cryptocurrencies

## Private and Public Keys

- Employs asymmetric cryptography and cryptographic hash function
- Participant identity = blockchain address
- Public key → hash function → blockchain address

BTC: 1GK67bPQuCErckdhmCABg8esmHfqc32cih  
ETH: 0x71ffddd44c3a1d68ed129aa6ef7fd6f55d7f8804 } pseudo-anonymous

- Process to generate Bitcoin address:



# Types of Users

- Exchanger
- User

# Custodial vs. Non-custodial

- Exchanger = Virtual Asset Service Provider (VASP)
  - Over the Counter Exchanges (Coinbase, Gemini, Kraken)
  - Peer to Peer (e.g., DEX, localbitcoins.com, localcryptos.com)
  - Derivatives (LedgerX, Deribit.com)
  - Bitcoin/Crypto ATMs
  - Mixers and Tumblers
- The VASP manages the users' private keys.
- Have significant information on the users through KYC.

**VASP or Custodial provides the best approach from which crypto-assets can be seized through legal means such as seizure warrants.**

# Custodial vs. Non-custodial

- User = Someone who uses cryptocurrencies on their behalf
  - Retail investors and traders
  - Investment entities
  - Merchants
  - Miners and node operators
- The users manage their private keys.
- Has limited information the users.
- Usage of any VASP functions will expose user IP.\*

**De-anonymization of the user or account holder is more difficult because it requires more advance techniques including IP address and geolocation.**

# Know-Your-Customer (KYC) Process

ed.

Reducing  
AML risks



Assess customer risk and comply with Anti-Money Laundering (AML) laws.



Tier 1 – Identity Verification



Tier 2 – Proof of Address



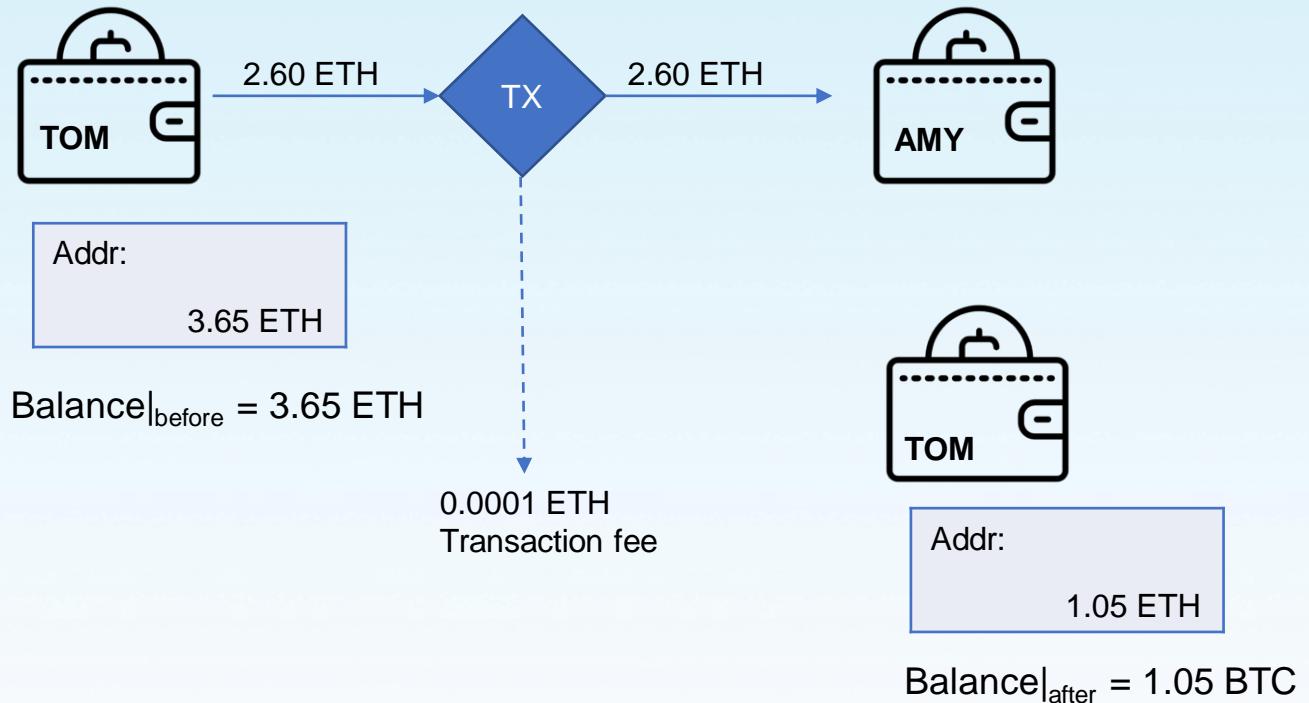
Tier 3 – Proof of Funds

# Controls for KYC and AML

- Know who are your customers.
  - Name
  - Date of birth
  - Address
  - Identification number
- What due diligence has been conducted?
  - Simplified Due Diligence
  - Basic Customer Due Diligence
  - Enhance Due Diligence
- Perform ongoing monitoring.

# Accounting Models

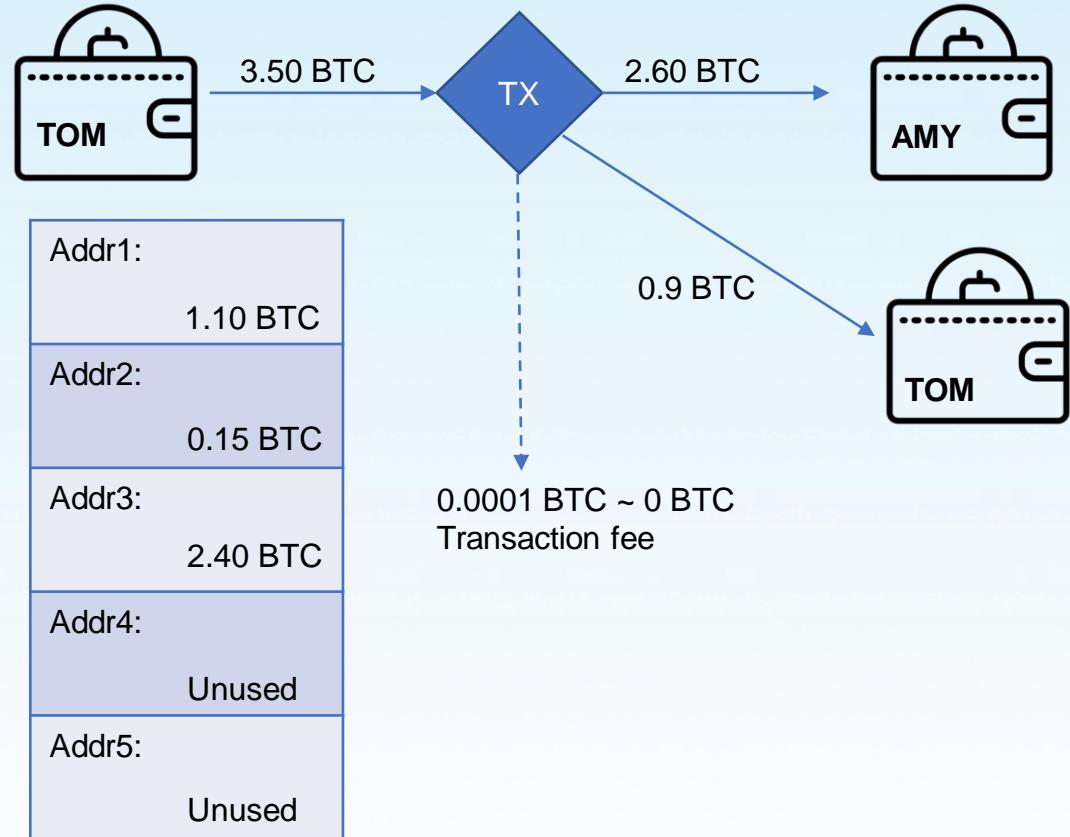
## Account-Balance Model



A single address is used for both sending and receiving cryptocurrencies and tokens. Easiest to track and identify user or account holder.

# Accounting Models

## Unspent Transaction Output (UTXO) Model



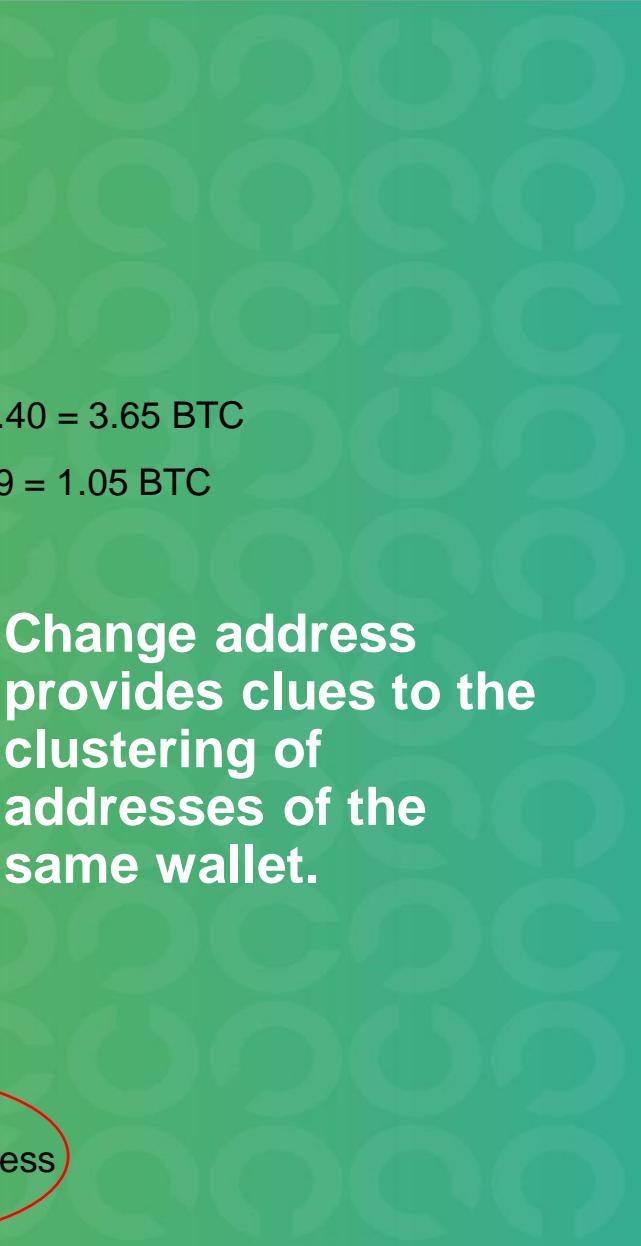
### Tom's Balance

$$\text{Balance}_{\text{before}} = 1.10 + 0.15 + 2.40 = 3.65 \text{ BTC}$$

$$\text{Balance}_{\text{after}} = 0 + 0.15 + 0 + 0.9 = 1.05 \text{ BTC}$$

|        |          |
|--------|----------|
| Addr1: | 0 BTC    |
| Addr2: | 0.15 BTC |
| Addr3: | 0 BTC    |
| Addr4: | 0.9 BTC  |
| Addr5: | Unused   |

← Change Address



# Cryptocurrency Investigation Basics

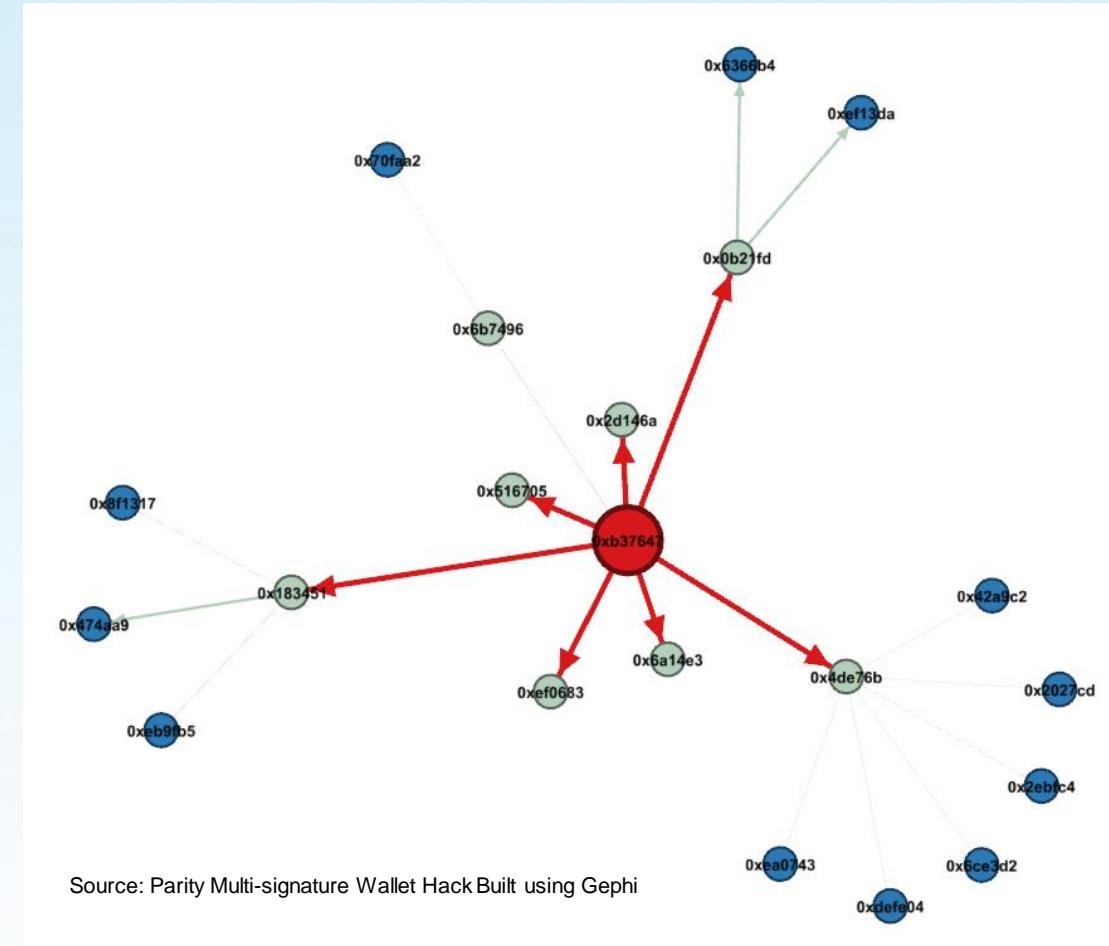
## 1. Follow The Money

- Transaction graph analysis
- Investigation tool to trace transactions
- Sankey diagram

## 2. Use address clustering heuristics to group addresses into related clusters.

## 3. Leverage attribution tags to de-anonymize the actor or account holder or other key addresses.

## 4. Identify key transactions and addresses for further legal actions or monitoring.

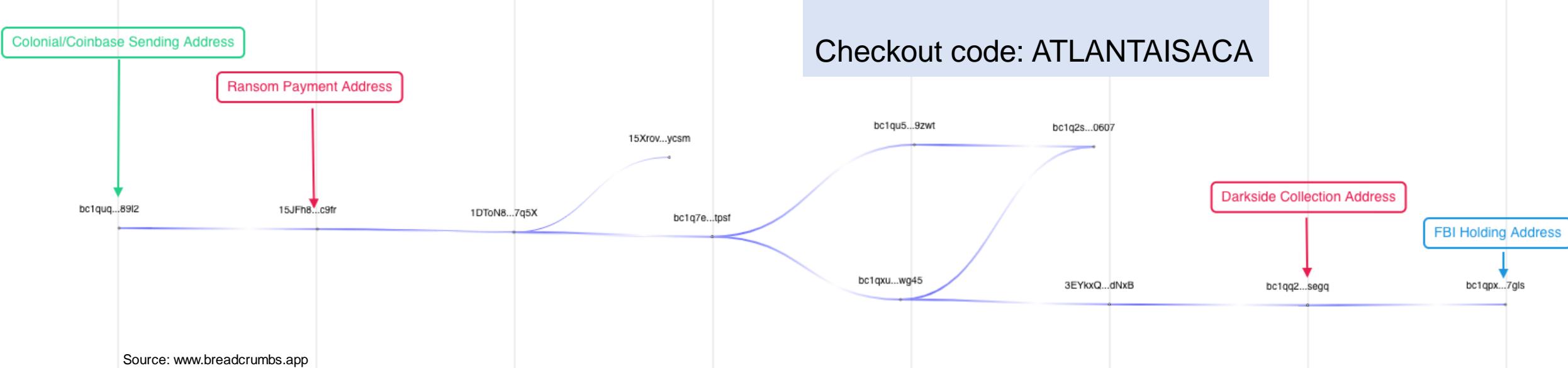


# Follow The Money

Colonial Pipeline Hack using Breadcrumbs.app

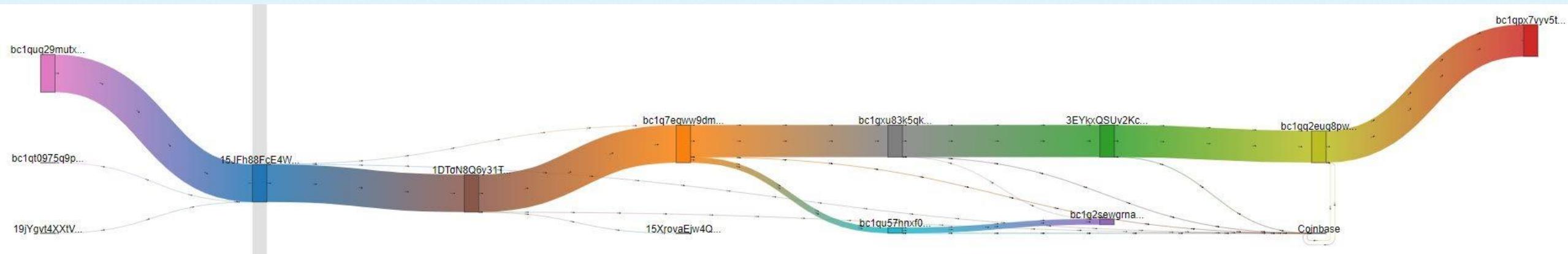
**Sign-up at Breadcrumbs.app  
at no cost for 30 days**

Checkout code: ATLANTAISACA



# Follow The Money

Colonial Pipeline Hack using Sankey Diagram



Source: bitquery.io

# Address Clustering Heuristics

Example #1 Change Heuristic: Single Input/Single Output

The screenshot shows a transaction details page from Blockchair.com. At the top left is the transaction hash: **28cb270e ... 908d7ab4**. To the right is a green circular icon with a checkmark, indicating the transaction is **Confirmed** with **597 confirmations** and a block id of **691,927**. Below the hash, the amount transacted is listed as **158.46068042 BTC** or **4,747,800.00 USD**. The transaction fee is **0.005 BTC** or **149.81 USD**. The fee per vbyte is **2,212 satoshi**. The transaction occurred **4 days ago**, on **Jul 21, 2021 12:18 AM UTC**. On the left side, there's a "Privacy-o-meter" icon showing a shield with a red gradient, labeled "Privacy" and "Critical". It also indicates there are **2 issues**. The main table shows one sender (**1FzWLkAa**) and two recipients (**1P5ZEDWT** and **1FzWLkAa**). The total input and output amounts are both **158.46068042 BTC** or **4,747,796.90 USD**.

| Senders                              | Recipients                      |
|--------------------------------------|---------------------------------|
| 1FzWLkAa                             | 1P5ZEDWT                        |
| 158.46068042 BTC<br>4,909,580.00 USD | 156.00 BTC<br>4,674,070.00 USD  |
|                                      | 1FzWLkAa                        |
|                                      | 2.46068042 BTC<br>73,726.90 USD |

Source: Blockchair.com

One of the recipient addresses is the same sender address.

The other recipient address may be the address of interest.

# Address Clustering Heuristics

## Example #2 Multi-Inputs: Co-spending

Transaction hash  
daf38c7b38eb0a587cf843f  
47000d5c294afbf4f560173  
70ad48c5147f5e69d9 

Amount transacted ?  
69.60422177 BTC -  
2,679,140.00 USD

Transaction fee ?  
0.00989322 BTC - 380.80 USD

Fee per vbyte  
140 satoshi

2 months ago ·  
May 28, 2021 3:06 AM UTC

Privacy  
 0 Critical ?  
Issues: 4

Privacy-o-meter shows the level of traceability of a transaction via various tracking tools

Transaction status  
Confirmed · 11,020 confirmations   
Block id 685,213

Additional info  Transaction receipt 

| Senders 24  | Recipients 1  |
|---|---|
| 378JHJCpWgSKKLzBMY3gm9eN7erGJF<br>3Qeh <br>← 0.00164331 BTC - 92.86 USD    | bc1qq2euq8pw950klpjcauwuy4uj39y<br>m43hs6cfsegq <br>69.60422177 BTC - 2,679,140.00 USD  |
| 3E71mBDDXxkk1W4Ubz4vq6cQwNism5<br>wr0r <br>← 0.000021 BTC - 0.14 USD       |   |
| 33EPYRGgMjEs1Vgvz2Fe8Cikc3yCSe<br>kSEK <br>← 0.000001 BTC - 0.33 USD       |   |
| 3QP3qP JqTHvXdvrTEDM79UQwBo7wpw<br>toYg <br>← 0.000001 BTC - 0.33 USD    |   |
| 3FfgjyWERGVxtgBvohVnTbjCWL6u4h9<br>YqRQ <br>← 0.00055095 BTC - 26.12 USD |   |
| 3GvGXyDg59JU38aVhQJncYH2zwtEn<br>QaUr <br>← 0.0000 BTC - 0.11 USD        |   |

Source: Blockchair.com

All inputs co-spent in  
the same transaction  
belong to the same  
wallet.

# Address Clustering Heuristics

Example #3 Transaction Type Fingerprinting (Type of Addresses)

The screenshot shows a transaction details page from Blockchair.com. The transaction hash is 5d326a35 287eff8f. The transaction status is "Waiting for confirmations - 0 of 6" with a "segwit" note. The queue position is 479 of 1395, and the estimated time to confirmation is 6 minutes. The amount transacted is 0.00430244 BTC (147.56 USD). The transaction fee is 0.0000033 BTC (0.11 USD). The fee per vbyte is 2 satoshi. The transaction was created 35 seconds ago on Jul 25, 2021, at 12:02 AM UTC. The privacy rating is "Moderate" (60) with 1 issue. The transaction has 1 sender and 2 recipients. The sender is bc1qnuyc...xk89qxj6, which spent 0.00430574 BTC (144.24 USD). The recipients are 3LnSwZZA...1YyQNaSF (0.00072998 BTC / 25.04 USD) and bc1qhqv7...mjyvgqtm (0.00357246 BTC / 122.52 USD). A callout box highlights "Three Types" of addresses used: Bech32 (bc1q...), P2PKH (1M3RLrXC...), and P2SH/Multi-Signature (3LnSwZZA...).

Transaction hash  
5d326a35 287eff8f

Amount transacted ?  
0.00430244 BTC • 147.56 USD

Transaction fee ?  
0.0000033 BTC • 0.11 USD

Fee per vbyte  
2 satoshi

35 seconds ago •  
Jul 25, 2021 12:02 AM UTC

Privacy  
60 Moderate ?  
Issues: 1

Privacy-o-meter shows the level of traceability of a transaction via various tracking tools

Transaction status  
Waiting for confirmations • 0 of 6 ? segwit

Queue: 479 of 1395 ⓘ Est. time to confirmation: in 6 minutes ?

Additional info Transaction receipt Notify me

Input total Output total  
0.00430574 BTC • 144.24 USD 0.00430244 BTC • 147.56 USD

Senders 1 Recipients 2

bc1qnuyc...xk89qxj6 0.00430574 BTC • 144.24 USD ⓘ

3LnSwZZA...1YyQNaSF ⓘ  
0.00072998 BTC • 25.04 USD

bc1qhqv7...mjyvgqtm ⓘ Change  
0.00357246 BTC • 122.52 USD

Source: Blockchair.com

Type of addresses provides clues of which output addresses may be the change address.

# Address Clustering Heuristics

Example #4 Multi-Inputs Heuristic: Multiple Inputs with Known Change Address

The screenshot shows a transaction detail page from Blockchair.com. At the top, it displays the transaction hash (ef3e8530 db758faf) and its status as confirmed with 27427 confirmations, block id 665,379. Below this, it shows the amount transacted (0.54599468 BTC - 22,075.10 USD), transaction fee (0.00113322 BTC - 45.82 USD), and fee per vbyte (102 satoshi). The transaction occurred 6 months ago, on Jan 10, 2021, at 7:12 AM UTC.

The privacy section indicates a critical level of traceability with 4 issues found. A red box highlights the "Senders" section, which lists seven input addresses. A second red box highlights the "Recipients" section, which shows two outputs: one to 1C8B2sHi...R7TpVtRT (0.48635852 BTC - 19,664.00 USD) and one to 12euiCot...iPokCgnG (0.05963616 BTC - 2,411.15 USD). The "Change" button next to the recipient address is also highlighted with a red box.

Source: Blockchair.com

Multiple inputs can be assumed to be from the same wallet.

Change address can be one of the input addresses.

# Address Clustering Heuristics

walletexplorer.com for Example #4

Wallet [0063f8dfbc] ([show transactions](#))

Page 1 / 2 [Last](#) (total addresses: 159)

| address   | balance    | incoming txs | last used in block |
|---|------------|--------------|--------------------|
| 1C8B2shizzdZ1ep5avhV3Qx2i4R7TpVtRT                  | 1.87983897 | 124          | 692562             |
| <a href="#">12euiCotw1o7XHM441Qfui7aLfiPokCgnG</a>  | 0.00528104 | 16           | 692562             |
| <a href="#">1CuZJEZ2Fu9ykR62ooGm8bi2GuMfiZoeDb</a>  | 0.         | 46           | 675581             |
| <a href="#">17NEz9fojCB9gX2YVdYkJLXYtvfm66tZVh</a>  | 0.         | 44           | 639481             |
| <a href="#">13fYZEkg4z3ffKANqw237J19he6j2JvfJB</a>  | 0.         | 20           | 625573             |
| <a href="#">13DMx7eLezj1sKxGwZzvdrVSh3LMcagbCQ</a>  | 0.         | 12           | 692562             |
| <a href="#">1PhHCnBFwAg4cjR8LbsTpKEHRBPravxV4c</a>  | 0.         | 11           | 675581             |
| <a href="#">1Mnp577SczacT4mLABrkZcSGC5JQKtr1Yo</a>  | 0.         | 10           | 692562             |
| <a href="#">1gPSMyC9qLEW6VELto8pA68iyV4x3Ly4T</a>   | 0.         | 9            | 619636             |
| <a href="#">151E7LjTvYZKFkhSnJ7vKaGED9vrkHtUMG</a>  | 0.         | 8            | 692562             |
| <a href="#">1J4QsoLUZhNAYnewB5aBoMMXYNACfxvySS</a>  | 0.         | 8            | 685475             |
| <a href="#">14s4FAe5Jc42juBP8zBac9wWPvrUxNcuT</a>   | 0.         | 8            | 678723             |
| <a href="#">1NnHEvwqU7yCFiDc4PakA3Q2P9DY4AAhmA</a>  | 0.         | 7            | 671974             |
| <a href="#">1CTaKsFaZJ41An9e2SJBmgeWhE4gkqxzdMZ</a> | 0.         | 6            | 670543             |
| <a href="#">152sGYVZ1h4FLKwDqorEXhn4J2MNLijgst</a>  | 0.         | 6            | 644954             |
| <a href="#">1Kqs26mmLrMuhcqapMSQZ2XE8kMMnSgRYq</a>  | 0.         | 6            | 633519             |
| <a href="#">1BM6nRArSrpaheBLwfoaoBvkGSpsR2GCVB</a>  | 0.         | 6            | 625573             |
| <a href="#">12ak8yAJRGj8BMUoh2NANYUMrhGYi4sxYz</a>  | 0.         | 6            | 619636             |
| <a href="#">1Jk8d7A85eurww6ZaGpWGwsALAZeUCstCv</a>  | 0.         | 6            | 601770             |
| <a href="#">1HHjKA6D17zaqPAheZRRCLKtvkU5jh8XYs</a>  | 0.         | 6            | 587956             |
| <a href="#">1SDTuuhxkJMNdwjdHAPpCefvdPWeoRT67</a>   | 0.         | 5            | 692562             |
| <a href="#">1G2NKHe8afMPwbUFZxGWY454C6Ksw6tPg</a>   | 0.         | 5            | 685475             |

Source: walletexplorer.com

# Address Clustering Heuristics

Example #5 Multi-Inputs Heuristic: Multiple Inputs with Unknown Change Address

The screenshot shows a transaction detail page from Blockchair.com. At the top left is the transaction hash **a38b1fe9** with a copy icon. To its right is the status **Confirmed** with **27801 confirmations**, a blue button for **segwit**, and a link to the **Block id 664,943**. Below the status are sections for **Additional info** and a **Transaction receipt**. Under the receipt, there are tables for **Input total** (0.01256756 BTC) and **Output total** (0.01244196 BTC). The **Senders** section (2 entries) and the **Recipients** section (4 entries) are highlighted with red and orange boxes respectively. The senders are **bc1qksuy** and **bc1qdxlf**, each receiving 0.00256756 BTC. The recipients are **bc1qyhsf**, **1FeeexV6b**, **bc1qpzfzu**, and **bc1lqr9dz**, each receiving 0.0001 BTC.

| Senders   | Recipients  |
|---|---|
| <b>bc1qksuy</b> ••• <b>prgml74d</b><br>0.00256756 BTC • 87.40 USD | <b>bc1qyhsf</b> ••• <b>xd73y3c8</b><br>0.0001 BTC • 3.69 USD  |
| <b>bc1qdxlf</b> ••• <b>tcjj3nmx</b><br>0.01 BTC • 340.42 USD      | <b>1FeeexV6b</b> ••• <b>GW9sb6uF</b><br>0.0001 BTC • 3.69 USD |

**Privacy**: 96 High (Issues: 1)

Privacy-o-meter shows the level of traceability of a transaction via various tracking tools

Source: Blockchair.com

Multiple recipients can make identification of change address more challenging.

# Address Clustering Heuristics

walletexplorer.com for Example #5

| Wallet [1fc13b452d] ( <a href="#">show transactions</a> )  |         |              |                    |
|--|---------|--------------|--------------------|
| address  | balance | incoming txs | last used in block |
| <a href="#">bc1qdxlfkcfjg065tfgdc94py0c05jgmkktcjj3nmx</a> | 0.      | 1            | 664943             |
| <a href="#">bc1qksuyh84l9q2xgy3ywzc5aqdkc0m6wqprgml74d</a> | 0.      | 1            | 664943             |
| Page 1 / 1 (total addresses: 2)                            |         |              |                    |

## Transaction a38b1fe985bf59de12324ace5005faa20cb57fad37fd6ff09909fe8728b3d2a8

|                   |  |
|-------------------|--|
| Txid              | a38b1fe985bf59de12324ace5005faa20cb57fad37fd6ff09909fe8728b3d2a8 |
| Included in block | 664943 (pos 2713)  |
| Time              | 2021-01-07 10:15:03  |
| Sender            | [1fc13b452d]   |
| Fee               | 0.0001256 BTC (28.81 satoshis/byte)                              |
| Size              | 436 bytes  |

| inputs: 2 (0.01256756 BTC)   | unique addresses: 2, source transactions: 2 | outputs: 4 (0.01244196 BTC)  | unique addresses: 4, spent: 3 in 3 transactions |
|--|---|--|---|
| 0. <a href="#">bc1qksuyh84l9q2xgy3ywzc5aqdkc0m6wqprgml74d</a> 0.00256756 BTC <a href="#">2a0f3fec...</a><br>1. <a href="#">bc1qdxlfkcfjg065tfgdc94py0c05jgmkktcjj3nmx</a> 0.01 BTC <a href="#">bbdc6fca...</a> |   | 0. <a href="#">bc1qyhsf9cl9wranc69u78hy3g6d4jhng5xd73y3c8</a> [5971ec44ba] 0.0001 BTC <a href="#">dac3854a...≡</a><br>1. <a href="#">1FeexV6bAHb8ybZjqQMjJrcCrHW9sb6uF</a> [cfe6738081] 0.0001 BTC unspent<br>2. <a href="#">bc1qpfzuq3zjgkt05mrmmjuheaftr2v33tzv302a76</a> [06a35fc70a] 0.00240476 BTC <a href="#">c898d484...≡</a><br>3. <a href="#">bc1qr9dzt9k4pqhpzkerear7ryl03qp66ssn67n97da</a> [5a03493fe7] 0.0098372 BTC <a href="#">7cd6064f...≡</a> |   |

Source: walletexplorer.com

# Limitation of Address Clustering Heuristics

- The reliability of clustering results is of uttermost importance for forensic investigations.
- Wrong clustering results can lead to missed or even false convictions.

## Common

- Multi-input heuristics – Addresses in transaction outputs redeemed in a multi-input transactions are controlled by the same entity.
- CoinJoin and similar trustless transactions – Causes multiple-input heuristic to produce false positives. Other examples of trustless transactions are Mixcoin, Blindcoin, CoinSwap, and CoinParty.

# Address Hunting using Partial Addresses

## Colonial Pipeline Ransom Hack

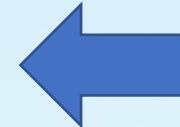
33. An online public blockchain explorer identified at least 23 other addresses collected together with address XXXXXXXXXXXXXXXRTnHQA8tNuG7S2pKedNxB in one wallet. [REDACTED] on May 27, 2021, funds from the collection of addresses, totaling 69.60422177 BTC, including 63.70000000 BTC accessible from address XXXXXXXXXXXXXXXRTnHQA8tNuG7S2pKedNxB was transferred to address XXXXXXXXXXXX950klpjcauwuy4uj39ym43hs6cfsegq (the "Subject Address"), and it has not moved since.

34. The private key for the Subject Address is in the possession of the FBI in the Northern District of California.

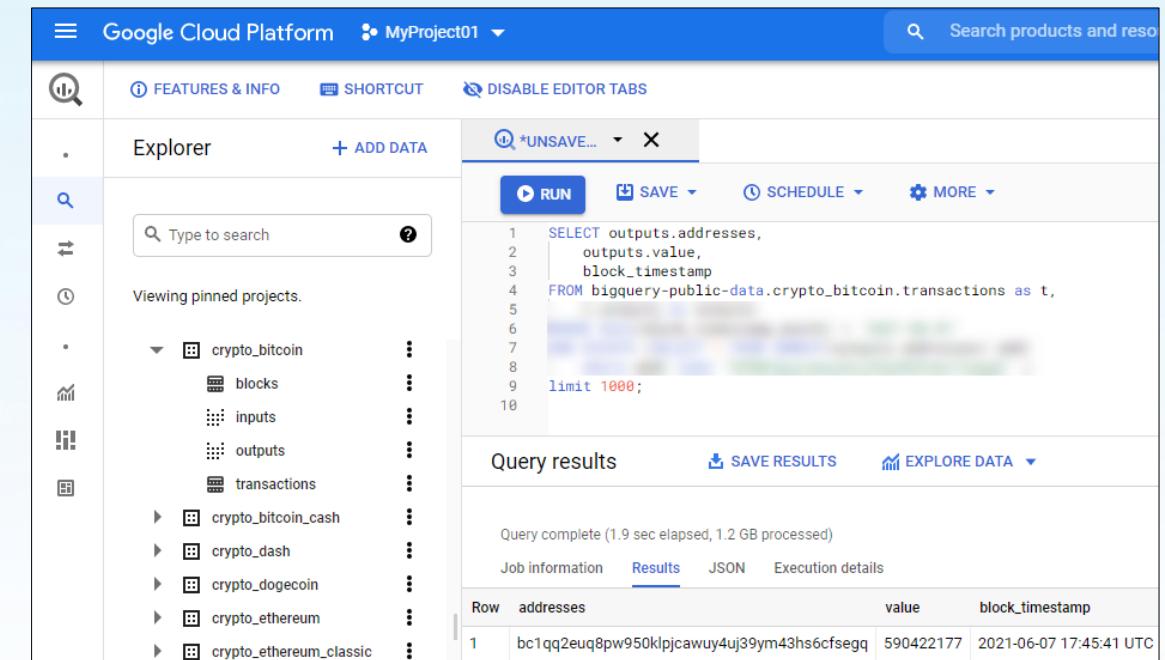
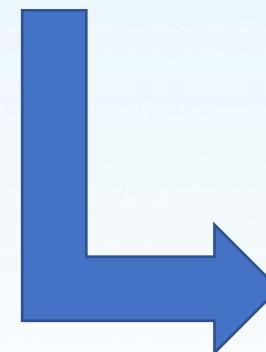
Source: [FBI's Seizure Warrant for Colonial Pipeline Hack](#)

Leverage Google's Bigquery for real-time search against public crypto datasets.

<https://cloud.google.com/bigquery>



The screenshot shows a news article from CNBC's Politics section. The headline reads: "Colonial Pipeline paid \$5 million ransom one day after cyberattack, CEO tells Senate". The article was published on Tuesday, June 8, 2021, at 10:17 AM EDT, and last updated on Wednesday, June 9, 2021, at 8:24 AM EDT.



The screenshot shows the Google Cloud Platform BigQuery interface. The user is in the "MyProject01" project. The interface includes a sidebar with project navigation, a search bar, and a main area for querying data. A specific query is run:

```
1 SELECT outputs.addresses,
2    outputs.value,
3    block_timestamp
4 FROM `bigquery-public-data.crypto_bitcoin.transactions` AS t,
5
6
7
8
9 LIMIT 1000;
```

The results of the query are displayed in a table:

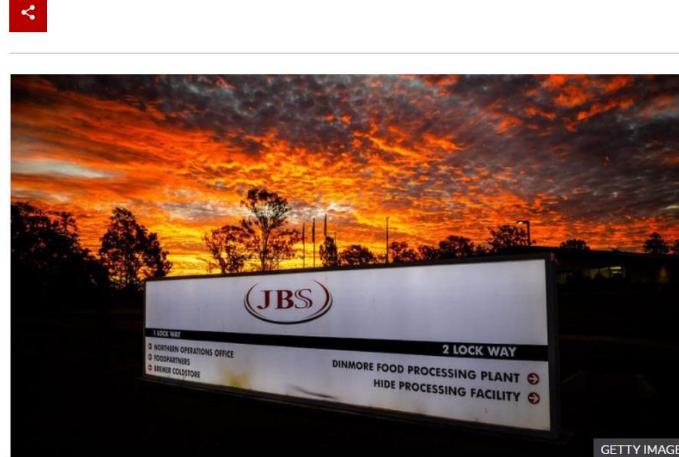
| Row | addresses                                   | value     | block_timestamp         |
|-----|---|-----------|-------------------------|
| 1   | bc1qq2euq8pw950klpjcauwuy4uj39ym43hs6cfsegq | 590422177 | 2021-06-07 17:45:41 UTC |

# Address Hunting using Specific Conditions

## JBS Ransom Hack

Meat giant JBS pays \$11m in ransom to resolve cyber-attack

© 10 June



The world's largest meat processing company has paid the equivalent of \$11m (£7.8m) in ransom to put an end to a major cyber-attack.

Computer networks at JBS were hacked last week, temporarily shutting down some operations in Australia, Canada and the US.

The payment was reportedly made using Bitcoin after plants had come back online.



The screenshot shows the Google Cloud Platform BigQuery interface. The top navigation bar includes 'Google Cloud Platform', 'MyProject01', and a search bar. The main area is titled 'Explorer' and shows a tree view of datasets like 'crypto\_bitcoin', which contains tables for 'blocks', 'inputs', 'outputs', and 'transactions'. A specific query is running in a window titled '\*UNSAVE...':

```
1 SELECT outputs.addresses,
2      outputs.value,
3      block_timestamp
4 FROM bigquery-public-data.crypto_bitcoin.transactions AS t,
5
6
7
8 limit 1000;
```

The results section shows the output of the query:

| Row | addresses                          | value       | block_timestamp         |
|-----|------------------------------------|-------------|-------------------------|
| 1   | 1NmcvEH2rMeXaw3C9mkLhc3QkjV2AyNbLg | 30100000000 | 2021-06-01 23:20:00 UTC |
| 2   | 3L7ECcRBcypxrS5U9Kw9WexcsHmX4wKYz6 | 30100000000 | 2021-06-01 23:25:38 UTC |
| 3   | 1PdGND2KXZprBxoH5fs3yEp8gWzNLToGBB | 30100000000 | 2021-06-30 18:47:53 UTC |
| 4   | 38Vkp5DM9gTeWWZrrAo3e92oPK98yrHxAG | 30100000000 | 2021-06-25 05:11:31 UTC |

# Hunting for Specific Conditions

## JBS Ransom Hack - Analysis

| Row | addresses                          | value       | block_timestamp         |
|-----|------------------------------------|-------------|-------------------------|
| 1   | 1NmcvEH2rMeXaw3C9mkLhc3QkjV2AyNbLg | 30100000000 | 2021-06-01 23:20:00 UTC |
| 2   | 3L7ECcRBCypxrS5U9Kw9WexcsHmX4wKYz6 | 30100000000 | 2021-06-01 23:25:38 UTC |
| 3   | 1PdGND2KXZprBxoH5fs3yEp8gWzNLToGBB | 30100000000 | 2021-06-30 18:47:53 UTC |
| 4   | 38Vkp5DM9gTeWWZrrAo3e92oPK98yrHXaG | 30100000000 | 2021-06-25 05:11:31 UTC |

#1

  1NmcvEH2rMeXaw3C9mkLhc3QkjV2AyNbLg [Address](#) [Inflow](#) [Outflow](#) [Money Flow](#)

## Address Statistics

| Metric                      | Value      |
|-----------------------------|------------|
| Inputs in Transactions      | 1          |
| Outputs in Transactions     | 1          |
| First transaction date      | 2021-06-01 |
| Last transaction date       | 2021-06-01 |
| Received in Outputs         | 301 BTC    |
| Spent to Inputs             | 301 BTC    |
| Balance ( unspent outputs ) | 0 BTC      |

Total 7 rows

Source: bitquery.io

#2

  3L7ECcRBCypxrS5U9Kw9WexcsHmX4wKYz6 [Address](#) [Inflow](#) [Outflow](#) [Money Flow](#)

## Address Statistics

| Metric                      | Value      |
|-----------------------------|------------|
| Inputs in Transactions      | 1          |
| Outputs in Transactions     | 1          |
| First transaction date      | 2021-06-01 |
| Last transaction date       | 2021-06-01 |
| Received in Outputs         | 301 BTC    |
| Spent to Inputs             | 301 BTC    |
| Balance ( unspent outputs ) | 0 BTC      |

Total 7 rows

#3

  1PdGND2KXZprBxoH5fs3yEp8gWzNLToGBB [Address](#) [Inflow](#) [Outflow](#) [Money Flow](#)

## Address Statistics

| Metric                      | Value               |
|-----------------------------|---------------------|
| Inputs in Transactions      | 723                 |
| Outputs in Transactions     | 723                 |
| First transaction date      | 2019-09-11          |
| Last transaction date       | 2021-07-26          |
| Received in Outputs         | 114739.89793502 BTC |
| Spent to Inputs             | 114739.89793502 BTC |
| Balance ( unspent outputs ) | 0 BTC               |

Total 7 rows

#4

  38Vkp5DM9gTeWWZrrAo3e92oPK98yrHXaG [Address](#) [Inflow](#) [Outflow](#) [Money Flow](#)

## Address Statistics

| Metric                      | Value              |
|-----------------------------|--------------------|
| Inputs in Transactions      | 292                |
| Outputs in Transactions     | 294                |
| First transaction date      | 2020-10-01         |
| Last transaction date       | 2021-07-26         |
| Received in Outputs         | 92533.82467882 BTC |
| Spent to Inputs             | 92533.82466788 BTC |
| Balance ( unspent outputs ) | 0.00001094 BTC     |

Total 7 rows

[CSV](#) [JS](#) [GraphQL](#)

# Attributions

## Tagging

- Attribution = Linkage of address to real-life person, service, etc.
- How attributions are obtained
  - Honeypot
  - Self-reported
  - OSINT research
- How accurate are they?

# Attributions

Methods to Identify Attribution on Specific Addresses

- Google/Web searches
- Blockchain explorers
- API data calls
- Commercial blockchain investigation tools

# Attributions

Example

- Address: 32V6a7K46pSb1XQNGdrmdE2wjndVfJPet
- Tx Hash: 185ee32a4d768b2ad739f907447884b0ae9b435e009d791a5ec67b8bfc235974

Let's identify the attribution of the address!

# Attributions

bitinfocharts.com

Bitcoin Transaction 185ee32a4d768b2ad739f907447884b0ae9b435e009d791a5ec67b8bfc235974

Share:

block, address, transaction  Search

|                     |                              |
|---------------------|------------------------------|
| <b>Block</b>        | <b>582296</b>                |
| <b>Time</b>         | 2019-06-24 20:12:21          |
| <b>Size</b>         | 387 (bytes)                  |
| <b>Total Input</b>  | 433 BTC                      |
| <b>Total Output</b> | 432.99 <sub>002058</sub> BTC |
| <b>Fees</b>         | 0.00 <sub>037942</sub> BTC   |

← prev tx 32V6a7K46pSb1XQNGdrmdE2wjgndVfJPet -433 BTC  
wallet: BetVIP

|  |                             |
|--|-----------------------------|
| 12n3s8MCqdZzPnPisYrXagbfw8pJg8y9BW         | 300 BTC                     |
| bc1qpqtn46ndlme5ejurz3v33x79ku37v6m7nz0u   | 15 BTC                      |
| wallet: 51934323                           |                             |
| bc1qmftdfx6xxkju36e8xuncfl6a967jqgp6uuza7l | 15 BTC                      |
| wallet: 51934323                           |                             |
| bc1q9seyqfwzt8zkuurqcz4ghpzge7ettz6x2vq75a | 15 BTC                      |
| wallet: 51934323                           |                             |
| bc1q9266jp27jwf2nzpszp4mgyraduynql4r0s7zcj | 15 BTC                      |
| wallet: 51934323                           |                             |
| bc1qu4rv5lm5mwhrusva2je8u7vsh0kdvzw9n2r7e  | 15 BTC                      |
| wallet: 51934323                           |                             |
| bc1qqk6fl03h2anhcnvfzs2c3uqvmlj4reprk77    | 15 BTC                      |
| wallet: 51934323                           |                             |
| bc1qzk9l0t2zyjsz82dlxclwvy0fqethpm4yy38xc  | 15 BTC                      |
| wallet: 51934323                           |                             |
| bc1qsgz3ytwxpsgzukfrv89zkjwzgqwvtyrzv9u8n  | 15 BTC                      |
| wallet: 51934323                           |                             |
| bc1q02jxxwnwdq859j2nhylw6fy8m9sa38gjtv03jr | 12.99 <sub>002058</sub> BTC |

Fee: 0.00<sub>037942</sub> BTC

Source: bitinfocharts.com

Transaction sum: 432.99<sub>002058</sub> BTC

# Attributions

whale-alert.io



```
{  
  result: "success",  
  count: 10,  
  transactions: [  
    {  
      blockchain: "bitcoin",  
      symbol: "btc",  
      id: "204819897",  
      transaction_type: "transfer",  
      hash: "185ee32a4d768b2ad739f907447884b0ae9b435e009d791a5ec67b8bfc235974",  
      from: {  
        address: "32V6a7K46pSb1XQNGdrmdE2wjgndVfJPet",  
        owner: "coinbase",  
        owner_type: "exchange"  
      },  
      to: {  
        address: "12n3s8MCqdZzPnTisYrXagbfw8pJg8y9BW",  
        owner_type: "unknown"  
      },  
      timestamp: 1561421541,  
      amount: 300,  
      amount_usd: 3310393,  
      transaction_count: 1  
    },  
    + { ... },  
    + { ... },  
    + { ... },  
    + { ... },  
    + { ... },  
    + { ... },  
    + { ... },  
    + { ... },  
    + { ... }  
  ]  
}
```

## Transaction

Returns the transaction from a specific blockchain by hash. Blockchain inputs are: bitcoin, ethereum, ripple, neo, eos, tron and stellar. If a transaction consists of multiple OUTs, it is split into multiple transactions, provided the corresponding OUT is of high enough value (>=\$10 USD).

### HTTP Request

```
GET /v1/transaction/{blockchain}/{hash}
```

### URL Parameters

| Parameter  | Type   | Description  |
|------------|--------|--|
| blockchain | string | The blockchain to search for the specific hash (lowercase) |
| hash       | string | The hash of the transaction to return                      |

 Please note that a single hash can return multiple transactions for those blockchains that have multiple ins and outs per transaction or none at all if there are no valid inputs or outputs.

# Attributions

clankapp.com

clankapp.com/bitcoin/address/32V6a7K46pSb1XQNGdrmdE2wjgndVfJPet

clank

Bitcoin > (coinbase) 32V6a7K46pSb1XQNGdrmdE2wjgndVfJPet

Top 100 Richlist

|                                      |                                       |
|--------------------------------------|---------------------------------------|
| Balance<br><b>\$0.00</b><br>0.00 BTC | Total of transactions<br><b>5,031</b> |
|--------------------------------------|---------------------------------------|

Address balance is updated every hour. Last updated: 2021-07-31 20:40:39 ( now )

Last whales

Last biggest transactions involve this address.

| VALUE                              | SENDER                           | RECIPIENT                           | DATE                                     |
|------------------------------------|----------------------------------|-------------------------------------|--|
| <b>\$ 6,082,890</b><br>152.000 BTC | huobi<br>1KsFYJHLC1bSCRekPGzh... | coinbase<br>32V6a7K46pSb1XQNGdrm... | <b>1 day ago</b><br>2021-07-30 02:47:57  |
| <b>\$ 5,557,220</b><br>139.000 BTC | multiple addresses               | coinbase<br>32V6a7K46pSb1XQNGdrm... | <b>2 days ago</b><br>2021-07-29 01:00:24 |
| <b>\$ 1,488,880</b><br>38.000 BTC  | multiple addresses               | coinbase<br>32V6a7K46pSb1XQNGdrm... | <b>3 days ago</b><br>2021-07-28 16:52:15 |

Source: clankapp.com

# Attributions

walletexplorer.com

**Wallet [00000014ea]** ([show transactions](#))

First Previous... Page 267522 / 267522 (total addresses: 26,752,197)

| address   | balance | incoming txs | last used in block |
|---|---------|--------------|--------------------|
| <a href="#">1FZe3YGmEgWfrg9VmRPJL5bKcRYavi7XHF</a>  | 0.      | 1            | 194353             |
| <a href="#">1GEpgGPBvc7zs9sp7npQ1cvIBCLnsyyKqx</a>  | 0.      | 1            | 194353             |
| <a href="#">1J2AUr1PyKGoAjR6pjMFdc1tYJi9UVgw73</a>  | 0.      | 1            | 194353             |
| <a href="#">1JuMZ8jZdgZPn4Bs8q49mkZEJqfpv4msuH</a>  | 0.      | 1            | 194353             |
| <a href="#">1KS6ywvkBEsf53aivGhuzESMXHvsnxFrom5</a> | 0.      | 1            | 194353             |
| <a href="#">1DgtGU2PXi4iJQaHNbAcuGecjBGyJfJXC6</a>  | 0.      | 1            | 187760             |

First Previous... Page 267522 / 267522 (total addresses: 26,752,197)

**Address 1DgtGU2PXi4iJQaHNbAcuGecjBGyJfJXC6**

part of wallet [00000014ea]

Page 1 / 1 (total transactions: 2)

| date                | received/sent | balance | transaction  |
|---------------------|---------------|---------|--|
| 2012-07-06 08:38:31 | -0.1          | 0.      | <a href="#">e7f495e722ab47388051bcc19ec6371e2cb7d89952a29431ba80051d8ac7bf97</a> |
| 2012-07-06 06:33:36 | +0.1          | 0.1     | <a href="#">cc287a9790ab776da2e11250891e184e05b704535c2db65d2358213862712b41</a> |

Source: walletexplorer.com

About 20,900,000 results (0.61 seconds)

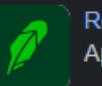
Coinbase / Founded

June 20, 2012

**coinbase**

People also search for

 Binance July 2017

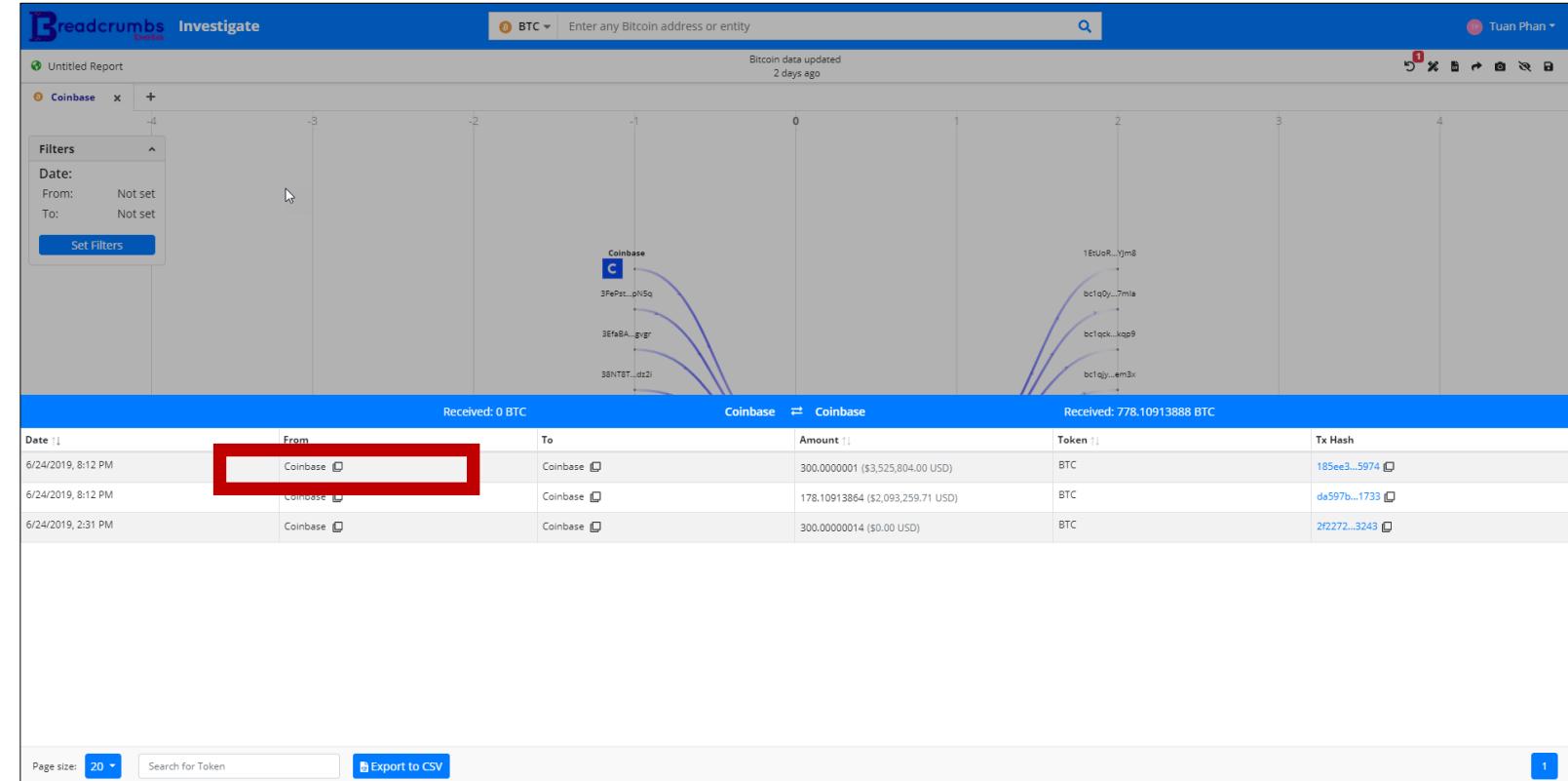
 Robinhood April 18, 2013

 Gemini 2014

Source: google.com

# Attributions

breadcrumbs.app



Source: breadcrumbs.app

# Tracking and Identifying Key Transactions

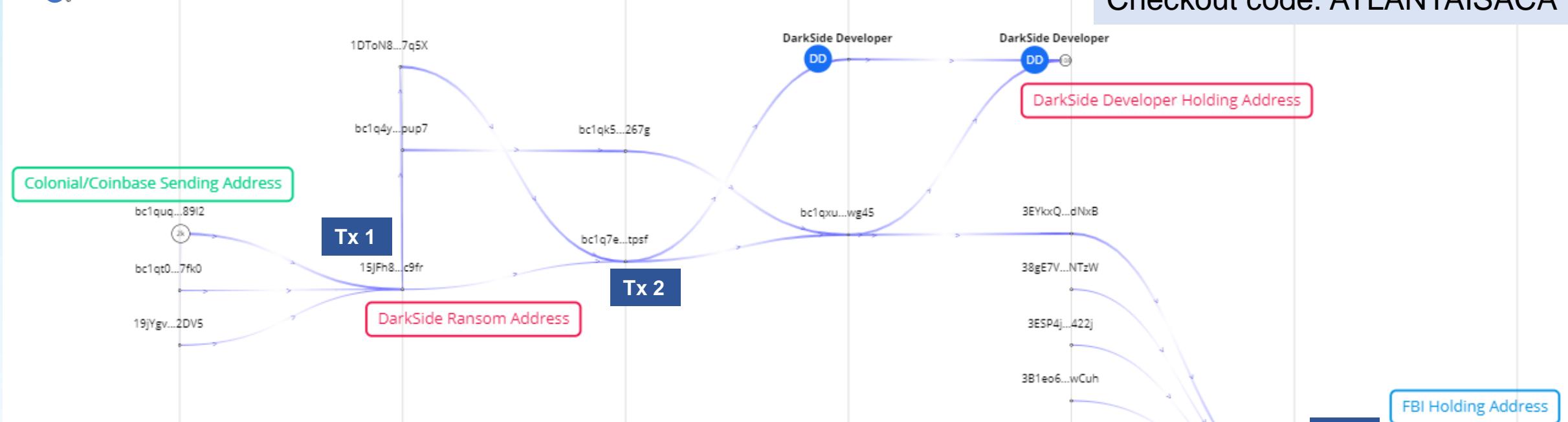
- Follow addresses with the largest received values starting from address of interest to point(s) of exit:
  - VASP exit points
  - Holding addresses (unspent addresses)
  - Mixers
  - Decentralized services (DeFi and related swap services)
- Transaction hashes provides the provenance information recorded.
  - Authenticity
  - Integrity
  - Reliability
- For seizure action, specific transaction hash must be specified.

# Tracking and Identifying Key Transactions

 [Colonial Pipeline Report on Breadcrumbs.app](#)

[Sign-up at Breadcrumbs.app](#)  
at no cost for 30 days

Checkout code: ATLANTAISACA



1. Payment from Colonial Pipeline to Ransom Address  
→ Tx `6a798026d44af27dbacd28ea21462808df8deca51794cec80c1b59e07ef924a2`
2. Distribution from Ransom as a Service  
→ Tx `0677781a5079eae8e5cbd5e6d9dcc5c02da45351a3638b85c88e5e3ecdc105a7`
3. FBI Seizure and Transfer into FBI Holding Address  
→ Tx `943f2d576ed8d9f388ba75eb82fe35cce29479b84121827ac368a5a94f44cf7a`

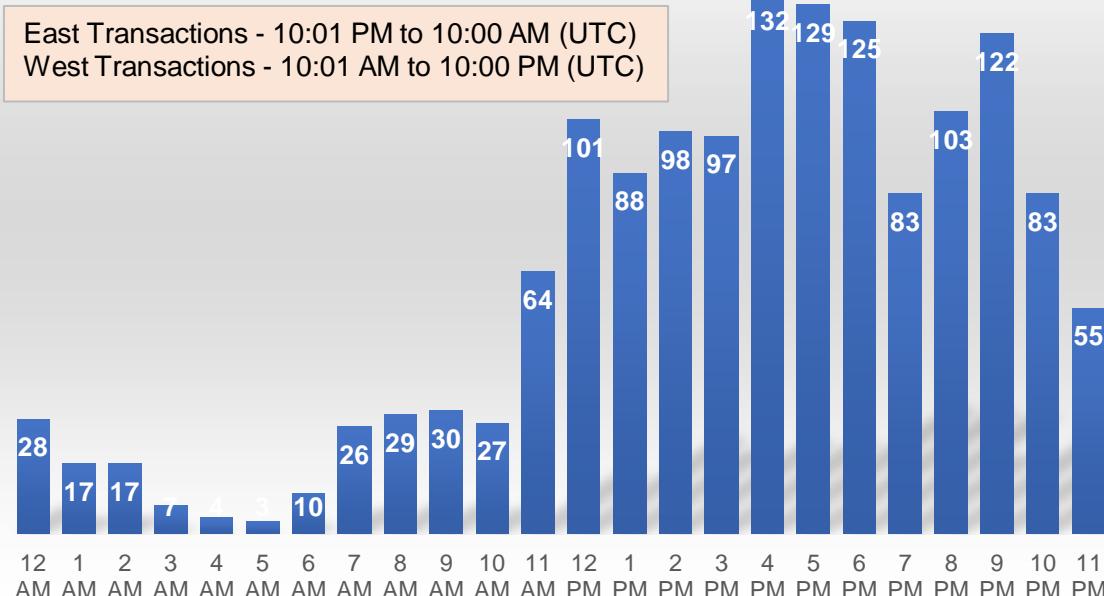
# Special Topics

- Transaction information such as date and time stamp to and from specific address can be clustered to determine:
  - Geographical region (Eastern or Western origination)
  - Day of week
- Specific (Bitcoin) IP of transactions can also be collected using earliest broadcast method.

# Geolocation using Transaction Timestamp

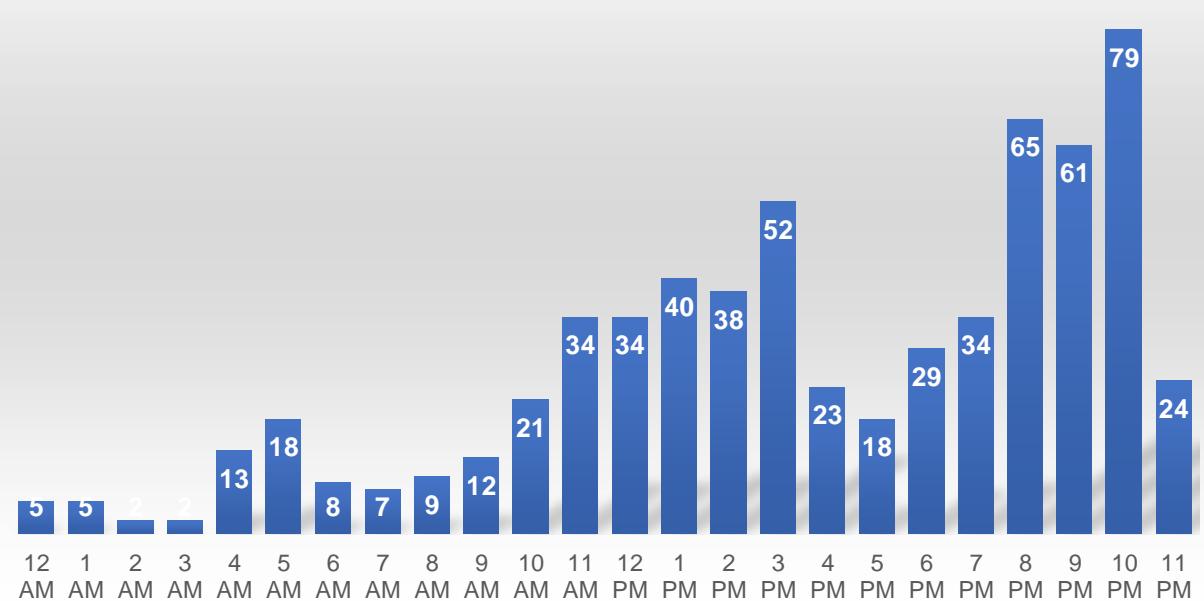
## Tether Exchange Scam

Approximate Geolocations of Victims using Inbound TXs



Most victims are from Western countries such as UK, Germany, and similar.

Approximate Geolocation of Scammer based on Outbound TXs



Likely to be based in Western countries as most transactions are between 10 AM and 10 PM.

# Identifying the Earliest Broadcast of Specific TX

Propagation of TXs to Peers on Bitcoin

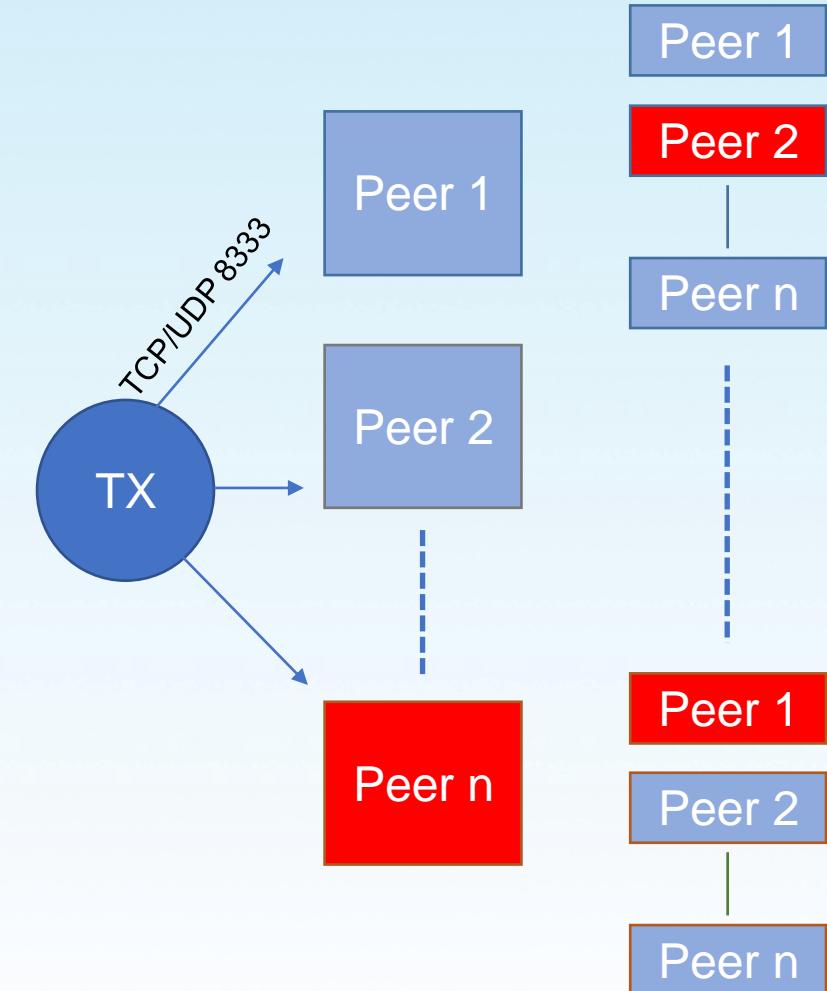
Node window

Information Console Network Traffic Peers

| NodeID | Node/Service          | Ping   | Sent  | Received | User Agent       |
|--------|-----------------------|--------|-------|----------|------------------|
| 0      | ↑ 192.69.53.70:8333   | 64 ms  | 1 KB  | 1 MB     | /Satoshi:0.21.1/ |
| 1      | ↑ 73.164.232.241:8333 | 319 ms | 1 KB  | 3 KB     | /Satoshi:0.21.1/ |
| 3      | ↑ 62.171.140.140:8333 | 249 ms | 22 KB | 185 KB   | /Satoshi:0.21.1/ |
| 6      | ↑ 35.236.147.169:8333 | 389 ms | 18 KB | 154 KB   | /Satoshi:0.20.1/ |
| 9      | ↑ 165.22.233.194:8333 | 54 ms  | 12 KB | 103 KB   | /Satoshi:0.20.1/ |
| 13     | ↑ 194.180.110.10:8333 | N/A    | 6 KB  | 2 KB     | /Satoshi:0.21.0/ |
| 14     | ↑ 35.183.49.55:8333   | 114 ms | 4 KB  | 42 KB    | /Satoshi:0.20.1/ |
| 15     | ↑ 37.97.249.17:8333   | 104 ms | 2 KB  | 3 KB     | /Satoshi:0.21.1/ |
| 16     | ↑ 35.237.109.49:8333  | 47 ms  | 2 KB  | 1 KB     | /Satoshi:0.20.1/ |
| 17     | ↑ 47.94.243.77:8333   | 446 ms | 1 KB  | 30 KB    | /Satoshi:0.16.0/ |

62.171.140.140:8333 (node id: 3)  
via 50.206.65.238:56763

Permissions N/A  
Direction Outbound  
Version 70016  
User Agent /Satoshi:0.21.1/  
Services NETWORK & WITNESS & NETWORK\_LI  
Starting Block 696122  
Synced Headers 696122  
Synced Blocks 696122  
Connection Time 2 m 45 s  
Last Send 1 s  
Last Receive 0 s  
Sent 22 KB  
Received 185 KB  
Ping Time 249 ms  
Ping Wait N/A  
Min Ping 249 ms  
Time Offset -50 s  
Mapped AS N/A



# Identifying the Earliest Broadcast of Specific TX

## Colonial Pipeline Hack

### DATA PROPAGATION

Get inv propagation stats in milliseconds for a block or transaction broadcasted over 8 hours ago. Stats are calculated based on the inv arrival times (UNIX time in milliseconds) from the first 1000 nodes.

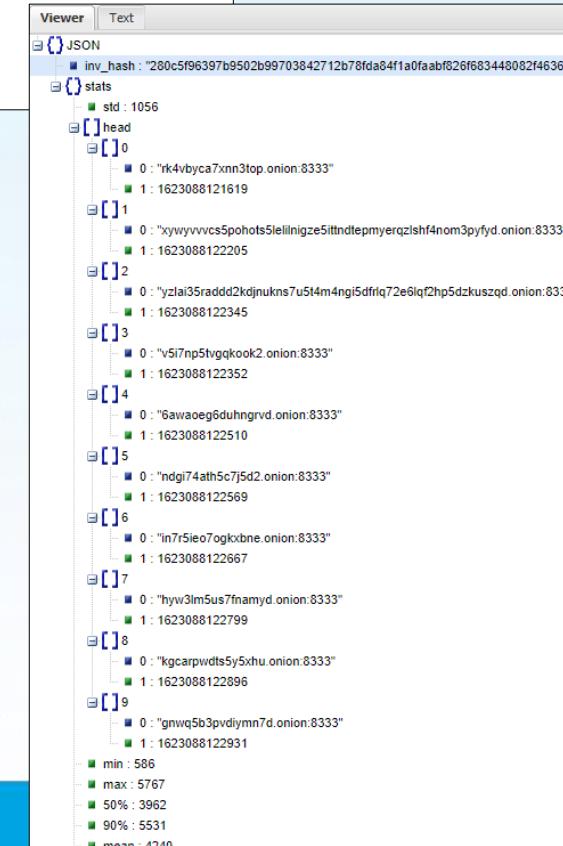
GET [https://bitnodes.io/api/v1/inv/<INV\\_HASH>](https://bitnodes.io/api/v1/inv/<INV_HASH>)

Values in stats represent the following information:

- head - Arrival times for the first 10 nodes in a list of ["<ADDRESS>:<PORT>", <TIMESTAMP>].
- min - Delta for earliest arrival time. Value can be 0 if the delta is less than 1 millisecond.
- max - Delta for latest arrival time.
- mean - Average of deltas.
- std - Standard deviation of deltas.
- 50% - 50th percentile of deltas.
- 90% - 90th percentile of deltas.



[Seizure by FBI](#)



[XFR 8 min later](#)

# Key Takeaways

- Learn about the various exchanges and the underlying risks for frauds and money laundering.
- With limitations, blockchain transactions can be de-masked to known entity using techniques including address clustering, attribution and others.
- Discuss and apply the tools and techniques to map and detail the flows of illicit transactions.
- Define the key controls for your organization to ensure compliance to KYC and AML and limit your exposure to the usage of cryptocurrencies for illicit transactions.

# Thank you!

Connect with me for any follow-up questions.

# Contact Information

Tuan Phan, CISSP, PMP, CTCE, CBSP, SSBB

Zero Friction LLC

+1 202-780-5455

[tphan@zerofriction.io](mailto:tphan@zerofriction.io)

@ChainOpSec

<https://www.linkedin.com/in/tuanphan/>



# Supplement Slides



# Retail Exchanges

- Offer cryptocurrency trading via an order book.
- Cater to new users to seasoned users.
- Custodial design
- Integrated built-in onramp for fiat-to-crypto
- Regulated - conforming to KYC and AML requirements
- Lowest risk of frauds or money laundering
- Higher fees



# Peer-to-Peer Exchanges

- Facilitate trades between individuals with the exchange as an escrow
- Use common payment methods such as Paypal, Venmo, credit cards, gift cards and other things of value of exchange
- Cater experienced users
- Non-custodial (some can be custodial)
- Does not have built-in onramp for fiat
- Greater chance for frauds and money laundering
- Lower fees



**LocalCoinSwap**

**LocalEthereum**

# Decentralized Exchanges

- Allow direct cryptocurrency transactions between two parties.
- Use smart contracts and protocols to handle transactions between user wallets.
- Typically for experienced users
- Non-custodial by design
- Independence from regulators – No verification of identity for KYC and AML
- Prone to market manipulation and frauds
- Fees between P2P and Retail Exchanges



IDEX



FORK  
DELTA

# Instant Exchanges

## – Type A :: Online

- Act as non-custodial cryptocurrency swap service providers.
- Provide easy to use and quick exchange from cryptocurrency key pairs
- Non-custodial by design
- Transitioning to KYC/AML compliant operating model
- Becoming less prone to money laundering
- Fees run between P2P and Retail Exchanges



# Instant Exchanges – Type B :: Mixers

- Act as non-custodial cryptocurrency swap service providers.
- Provide mixing of cryptocurrencies
- Non-custodial by design
- Independence from regulators – No verification of identity for KYC and AML
- Prone to money laundering
- Fees run between P2P and Retail Exchanges



CryptoMixer



# Instant Exchanges – Type C :: Offline

- Physical kiosks where one can connect cryptowallets and exchange for local currencies
- Non-custodial by design – Varying with country regulations
- Not all follow KYC and AML requirements
- Prone to money laundering
- Highest fees/commission level paid



# Instant Exchanges – Type C :: Offline

- Allow for future and option trading on cryptocurrencies.
- Provide easy to use and quick exchange from cryptocurrency key pairs
- Custodial by design



# Controls for KYC and AML

- Know who are your customers?
  - Name
  - Date of birth
  - Address
  - Identification number
- What due diligence has been conducted?
  - Simplified Due Diligence
  - Basic Customer Due Diligence
  - Enhance Due Diligence
- Perform ongoing monitoring

# Simplified to Enhanced Due Diligence

Controls for KYC and AML

- Ascertain the identity and location of the potential customers.
- Understand the customers' business income activities.
- Classify their risk category and define what type of customer they are, before storing this information and any additional documentation digitally.
- Conduct risk-based assessments considering the following factors:
  - Location of the person
  - Occupation of the person
  - Type of transactions
  - Source and pattern of activity in terms of transaction types, dollar value and frequency
  - Expected method of payment
- Maintain records performed on the customers.

# Ongoing Monitoring

Controls for KYC and AML

- Leverage risk scoring models to identify potentially:
  - Unusual spikes in activities
  - Out of area or unusual cross-border activities
- Adverse media mentions
- Interactions with blacklisted addresses or people/address on sanction lists
- Other best practices:
  - Is the account record up-to-date?
  - Do the type and amount of transactions match the stated purpose of the account?
  - Is the risk-level appropriate for the type and amount of transactions?