ISACA®
EMERGING TECH
VIRTUAL CONFERENCE
EVOLVE

Deconstructing the Colonial Pipeline Hack

Tuan Phan, CISSP, PMP, CTCE, CBSP, SSBB
Zero Friction LLC
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!

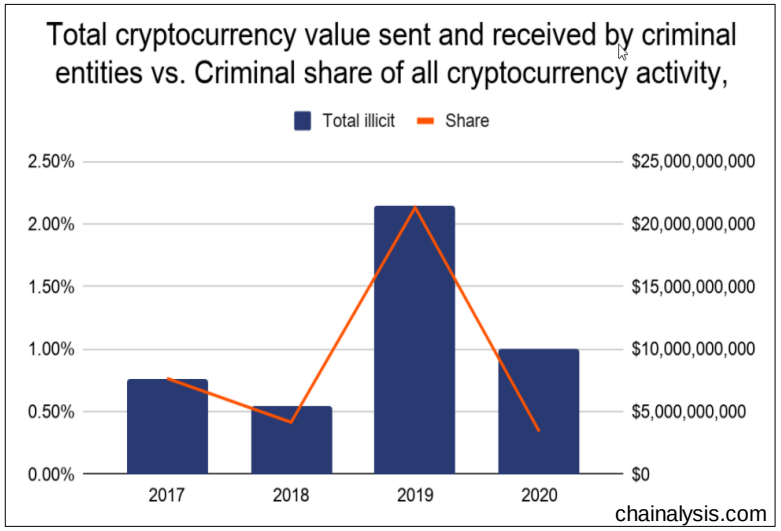
Don’t forget to fill out the session survey located within the mobile app after this and every session!

ISACA EMERGING TECH VIRTUAL CONFERENCE EVOLVE

Why do we conduct blockchain investigations

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

10 June



Menu Search **Bloomberg** Sign In **Subscribe**

Photographer: Samuel Corum/Bloomberg

Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

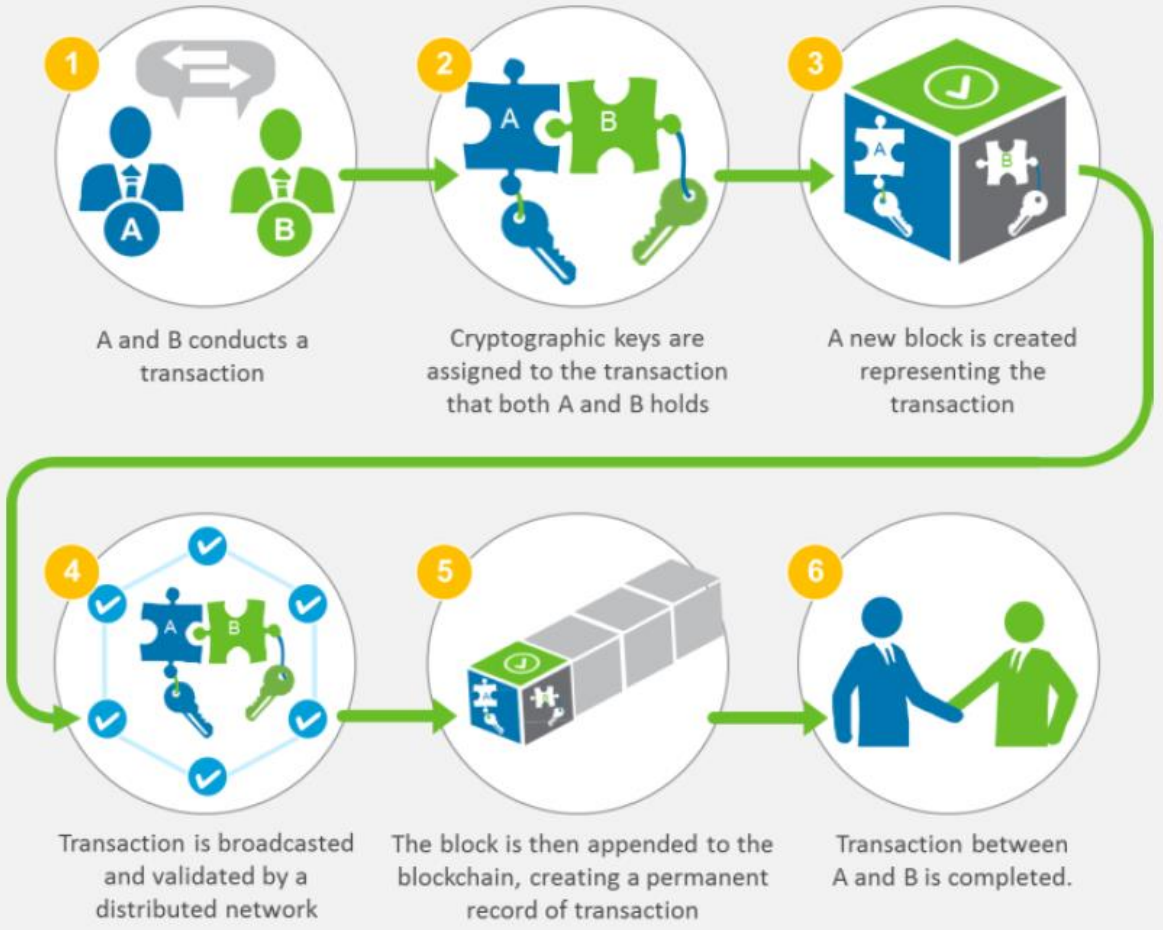
By William Turton and Kartikay Mehrotra
June 4, 2021, 3:58 PM EDT

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

LIVE ON BLOOMBERG
Watch Live TV
Listen to Live Radio

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).

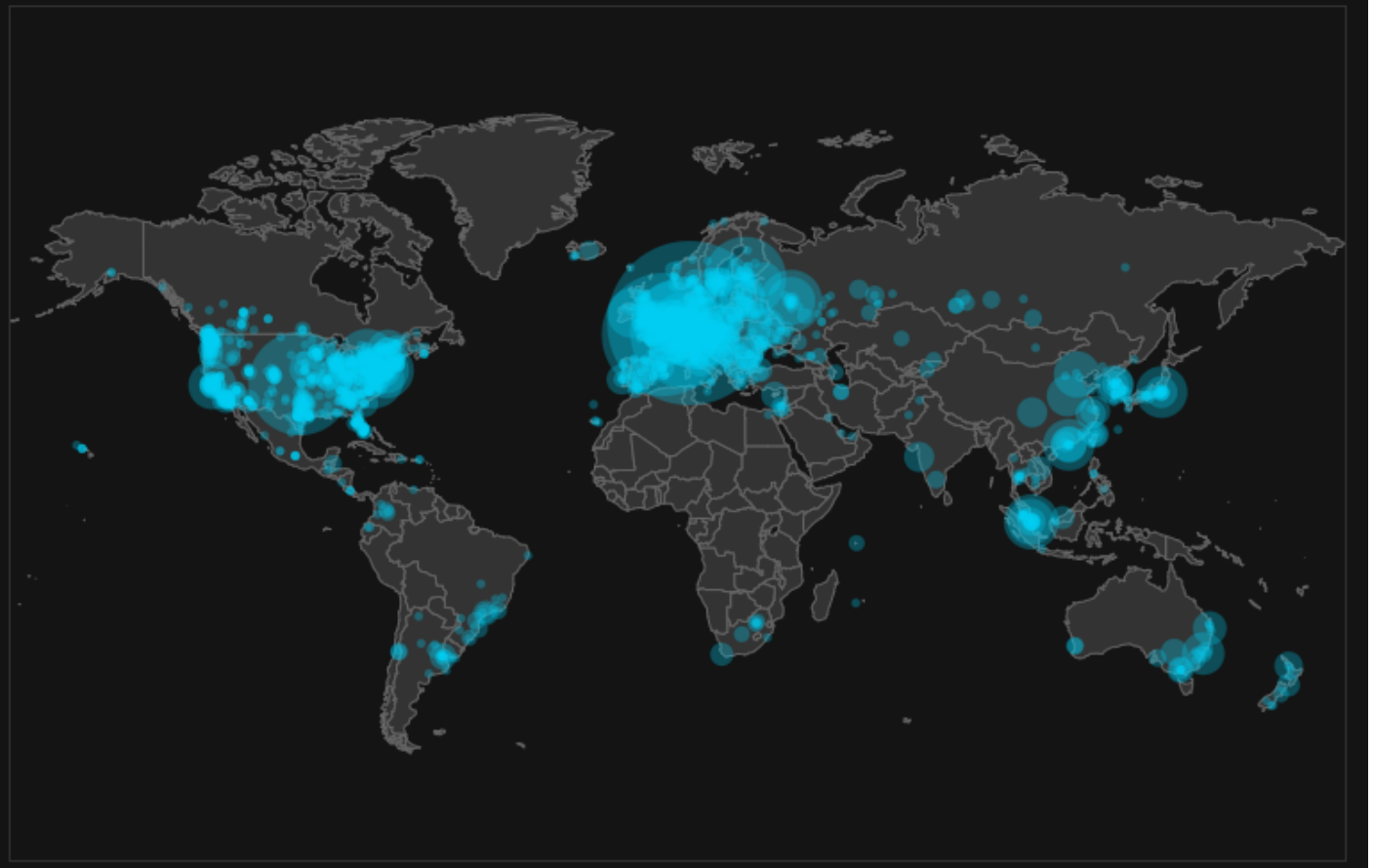
12307 NODES

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) »



Map shows concentration of reachable Bitcoin nodes found in countries around the world.

LIVE MAP

Identity Management of *Typical* Cryptocurrencies

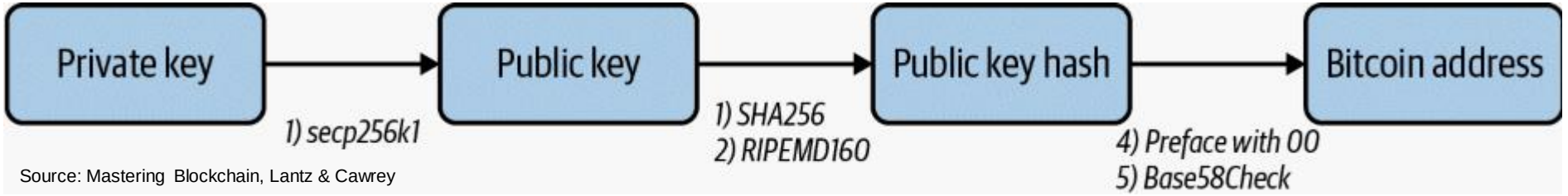
Private and Public Keys

- 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:



Source: Mastering Blockchain, Lantz & Cawrey

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

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

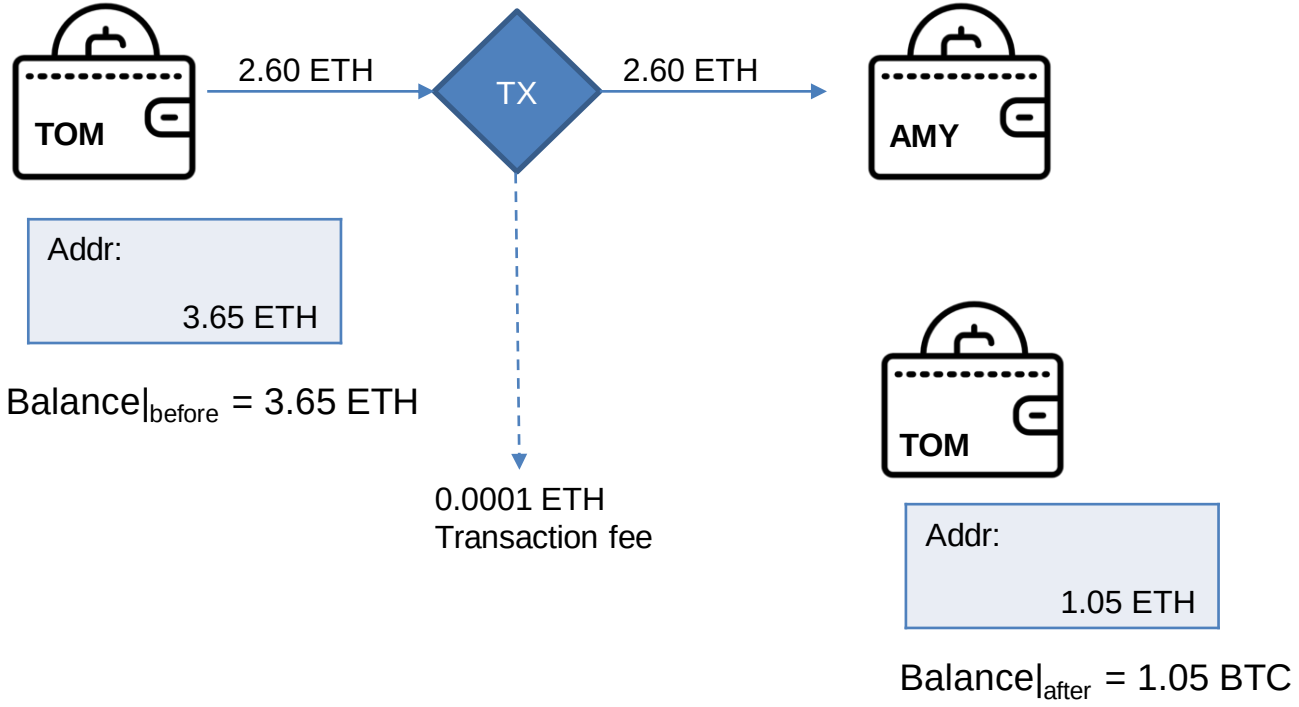
Reducing AML risks

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

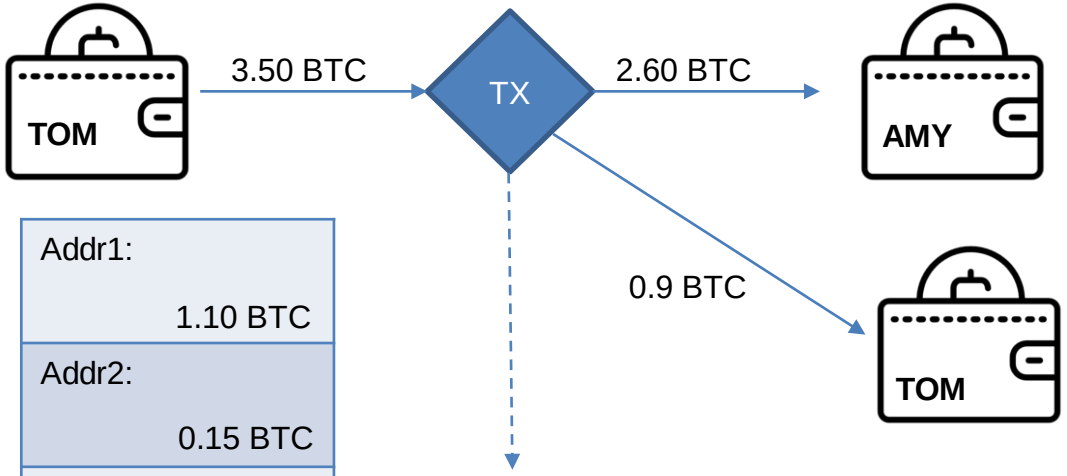
Account-Balance Model



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



Addr1:	1.10 BTC
Addr2:	0.15 BTC
Addr3:	2.40 BTC
Addr4:	Unused
Addr5:	Unused

Tom's Balance

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

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

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

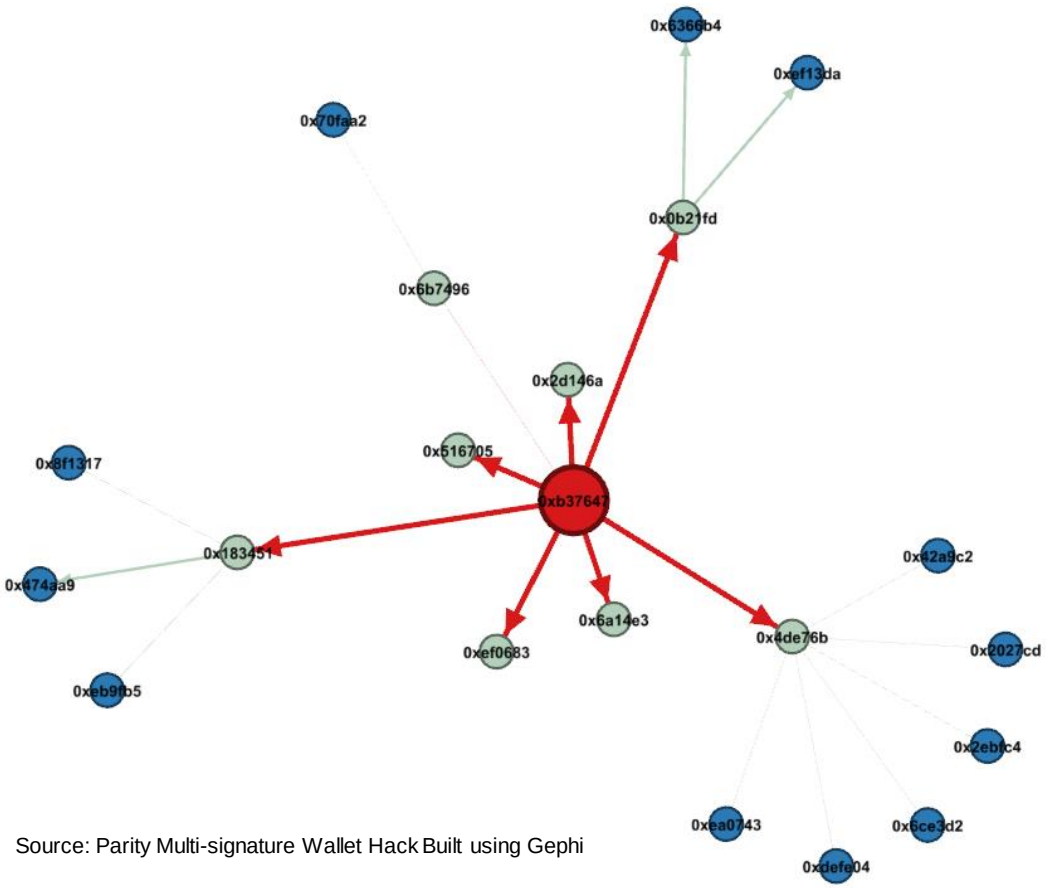
← Change Address

Change address provides clues to the clustering of addresses of the same wallet.

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.



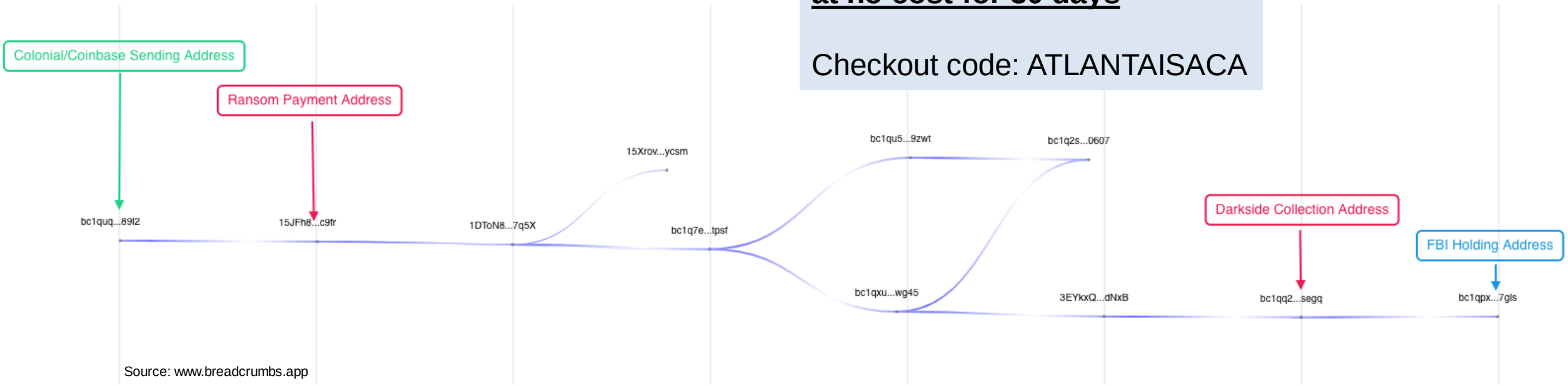
Source: Parity Multi-signature Wallet Hack Built using Gephi

Follow The Money

Colonial Pipeline Hack using Breadcrumbs.app

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

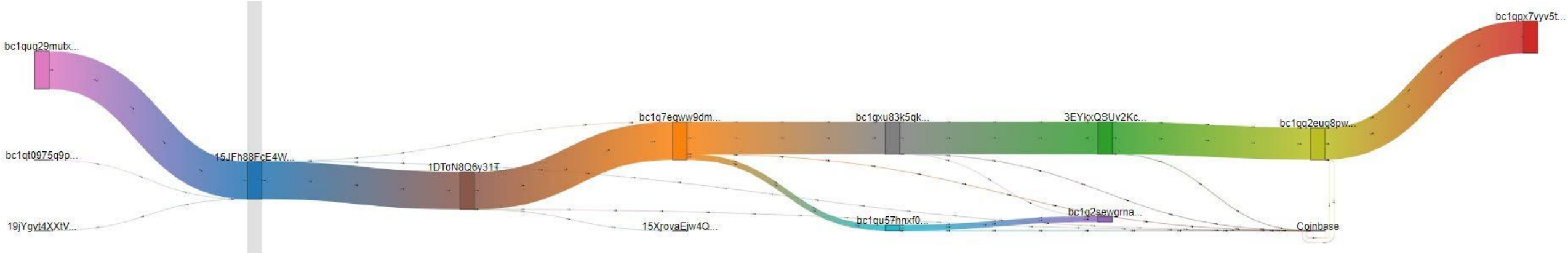
Checkout code: ATLANTAISACA



Source: www.breadcrumbs.app

Follow The Money

Colonial Pipeline Hack using Sankey Diagram



Source: bitquery.io

Address Clustering Heuristics

Example #1 Change Heuristic: Single Input/Single Output

Transaction hash

28cb270e ••• 908d7ab4

Amount transacted ?

158.46068042 BTC · 4,747,800.00 USD

Transaction fee ?

0.005 BTC · 149.81 USD

Fee per vbyte

2,212 satoshi

4 days ago · Jul 21, 2021 12:18 AM UTC

Privacy

0 Critical ?

Issues: 2

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

Transaction status

Confirmed · 597 confirmations ?

Block id 691,927

Additional info

Transaction receipt

Input total	Output total
158.46568042 BTC · 4,909,580.00 USD	158.46068042 BTC · 4,747,796.90 USD

Senders 1	Recipients 2
1FzWLkAa ••• J6sCXkSR 158.46568042 BTC · 4,909,580.00 USD	1P5ZEDWT ••• 54WKDfHQ 156.00 BTC · 4,674,070.00 USD
	1FzWLkAa ••• J6sCXkSR 2.46068042 BTC · 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

daf38c7b38eb0a587cf843f47000d5c294affb4f56017370ad48c5147f5e69d9

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

378JHJCpWgSKKLzBMY3gm9eN7erGJF3Qeh
0.00164331 BTC · 92.86 USD

3E71mBDDXxkk1W4Ubz4vq6cQwNism5wror
0.000021 BTC · 0.14 USD

33EPYRGgMjEs1Vgvz2Fe8Cikc3yCSekSEK
0.00001 BTC · 0.33 USD

3QP3qPJqTHvXdvrTEDM79UQwBo7wpwtoYg
0.00001 BTC · 0.33 USD

3FfgyWERGVxtgBvohVnTbjCWL6u4h9YqRQ
0.00055095 BTC · 26.12 USD

3GvGJXyDg59JU38aVhQJncYH2zwtEnQaUr
0.0000 BTC · 0.11 USD

Recipients 1

bc1qq2euq8pw950klpjcawuy4uj39ym43hs6cfsegq
69.60422177 BTC · 2,679,140.00 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)

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

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
0.00430574 BTC · 144.24 USD

Output total
0.00430244 BTC · 147.56 USD

Senders 1
bc1qnuyc•••xk89qxj6
0.00430574 BTC · 144.24 USD

Recipients 2
3LnSwZZA•••1YyQNasF
0.00072998 BTC · 25.04 USD

bc1qhpv7•••mjyvgqtm Change
0.00357246 BTC · 122.52 USD

Privacy
60 Moderate ?
Issues: 1

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

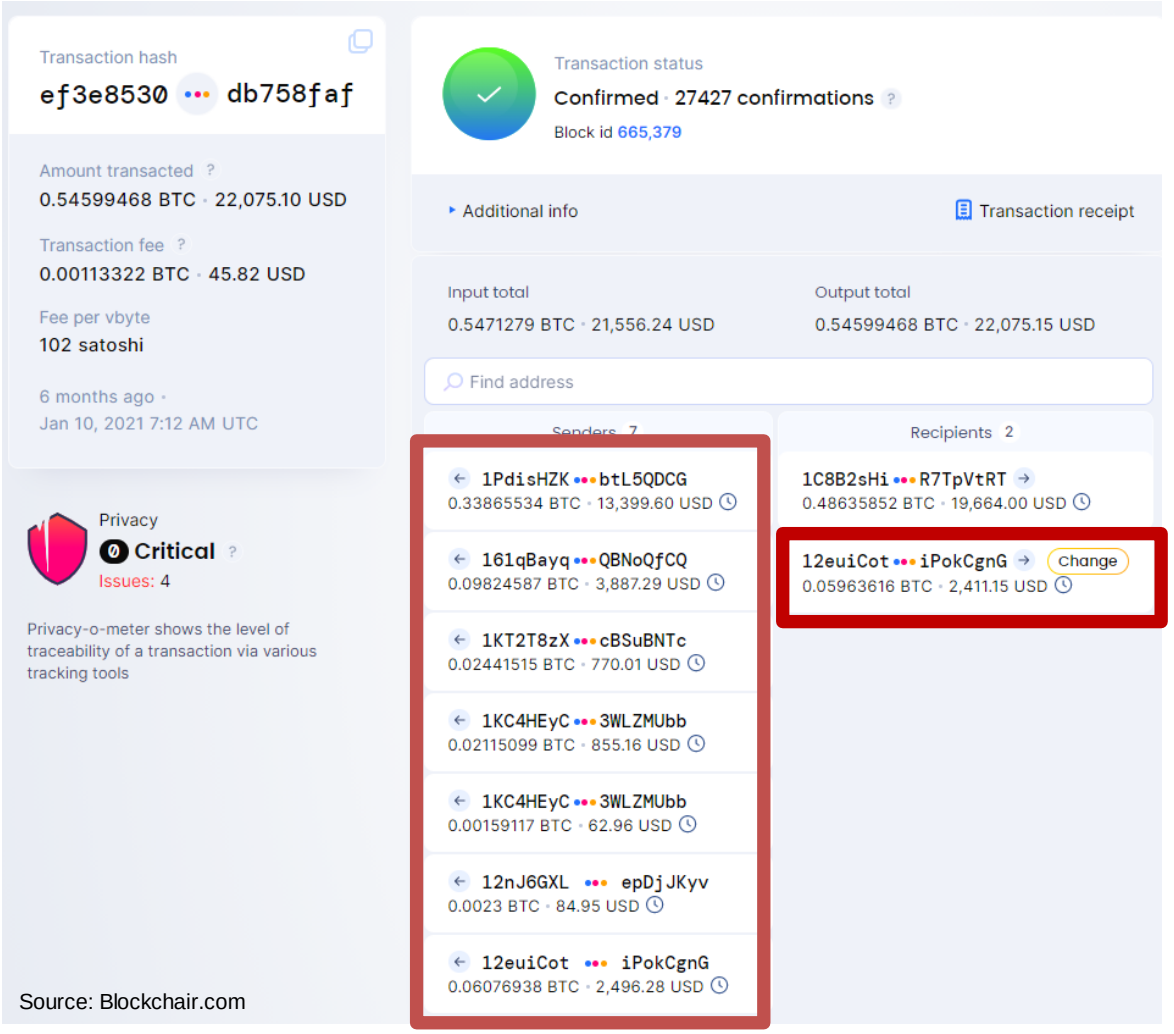
Three Types
- Bech32: bc1q…
- P2PKH: 1M3RLrXC…
- P2SH/Multi-Signature: 3LnSwZZA…

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



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
1C8B2sHizzdZ1ep5qvhV3Qx2i4R7TpVtRT	1.87983897	124	692562
12euiCotw1o7XHM441Qfui7aLfiPokCgnG	0.00528104	16	692562
1CuZJEZ2Fu9ykR62ooGm8bi2GuMfiZoeDb	0.	46	675581
17NEz9fojCB9gX2YVdYkJLXYtvfm66tZVh	0.	44	639481
13fYZEKg4z3ffKANqw237J19he6j2JvfJB	0.	20	625573
13DMx7eLezj1sKxGwZzvdrVSh3LMcagbCQ	0.	12	692562
1PhHCnBFwAg4cjR8LbsTpKEHRBPravxV4c	0.	11	675581
1Mnp577SczacT4mLABrkZcSGC5JQKtr1Yo	0.	10	692562
1gPSMyC9qLEW6VELto8pA68iyV4x3Ly4T	0.	9	619636
151E7LjTvYZKFkhSnJ7vKaGED9vrkHtUMG	0.	8	692562
1J4QsoLUZhNAYnewB5aBoMMXYNACfxvySS	0.	8	685475
14s4FAe5Jc42juBP8zBac9wWPvrUxNcuzT	0.	8	678723
1NnHEvwqU7yCFiDc4PakA3Q2P9DY4AAhmA	0.	7	671974
1CTaKsFaZJ41An9e2SJBmgeWhE4gkqxdMZ	0.	6	670543
152sGYVZ1h4FLKwDqorEXhn4J2MNLiJgst	0.	6	644954
1Kqs26mmLrMuhcqaPMSQZ2XE8kMMnSgRYq	0.	6	633519
1BM6nRArSrpaheBLwfoaoBvkGSpsR2GCVB	0.	6	625573
12ak8yAJRGj8BMUoh2NANYUMrhGYi4sxYz	0.	6	619636
1Jk8d7A85eurww6ZaGpWGwsALAZeUCstCv	0.	6	601770
1HHjKA6D17zaqPAheZRRLCKtvkU5jh8XYs	0.	6	587956
1SDTuuhxkJMNdwjdHAPpCefvdPWeoRT67	0.	5	692562
1G2NKHe8afMMPwbUFZxGWY454C6Ksw6tPg	0.	5	685475

Source: walletexplorer.com

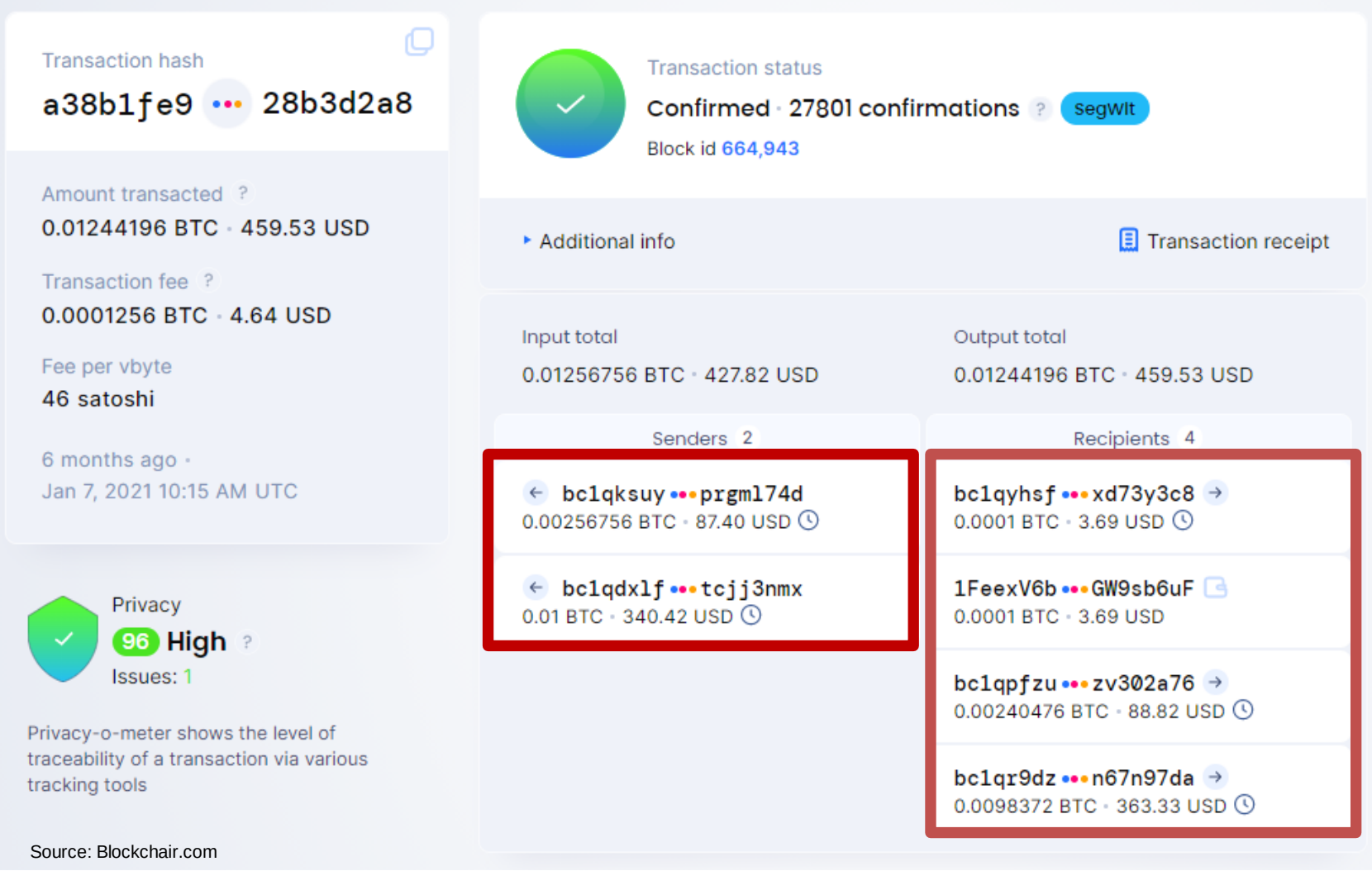
Clustering is the grouping of related addresses into a notional wallet:

1. Addresses are related if co-spent in one transaction:
   - A and B are spent in TX 1
   - B and C are spent in TX 2
   - A, B and C will consider part of the same wallet.

2. If change address is also an input address.

Address Clustering Heuristics

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



Source: Blockchair.com

Multiple recipients can make identification of change address more challenging.

Address Clustering Heuristics

walletexplorer.com for Example #5

Wallet [1fc13b452d] (show transactions)

Page 1 / 1 (total addresses: 2)

address	balance	incoming txs	last used in block
bc1qdxlfkcfjg065tfgdc94py0c05jgmkktcjj3nmx	0.	1	664943
bc1qksuyh84l9q2xgy3ywzc5aqdkc0m6wqprgml74d	0.	1	664943

Page 1 / 1 (total addresses: 2)

Transaction a38b1fe985bf59de1232 4ace5005faa20cb57fad37fd6ff09909fe8728b3d2a8

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

0.	bc1qksuyh84l9q2xgy3ywzc5aqdkc0m6wqprgml74d	0.00256756	BTC	⇐ 2a0f3fec...
1.	bc1qdxlfkcfjg065tfgdc94py0c05jgmkktcjj3nmx	0.01	BTC	⇐ bbdc6fca...

outputs: 4 (0.01244196 BTC) unique addresses: 4, spent: 3 in 3 transactions

0.	bc1qyhsf9cl9wranc69u78hy3g6d4jhng5xd73y3c8	[5971ec44ba]	0.0001	BTC	dac3854a... ⇒
1.	1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF	[cfe6738081]	0.0001	BTC	unspent
2.	bc1qpfzuq3zjgkt05mrrmjuheaftr2v33tzv302a76	[06a35fc70a]	0.00240476	BTC	c898d484... ⇒
3.	bc1qr9dzt9k4pqhpzkerea7ryl03qp66ssn67n97da	[5a03493fe7]	0.0098372	BTC	7cd6064f... ⇒

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.

<u>Common</u>

- 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

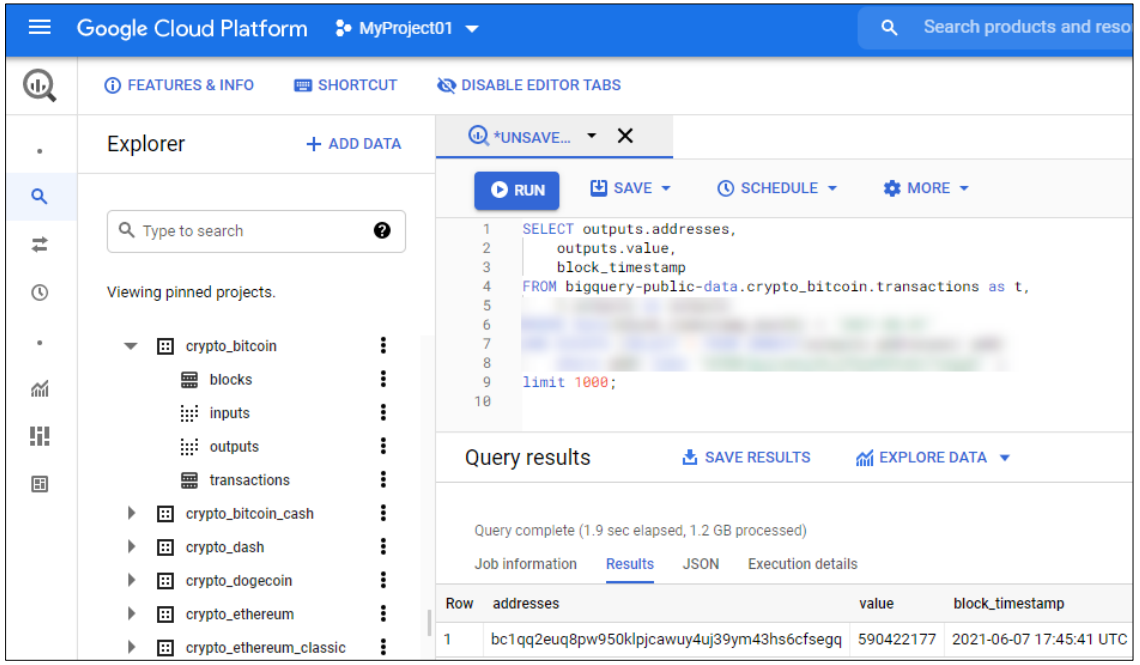
33. An online public blockchain explorer identified at least 23 other addresses collected together with address XXXXXXXXXXXXuRTnHQA8tNuG7S2pKedNxB in one wallet. [redacted] on May 27, 2021, funds from the collection of addresses, totaling 69.60422177 BTC, including 63.70000000 BTC accessible from address XXXXXXXXXXXXuRTnHQA8tNuG7S2pKedNxB was transferred to address XXXXXXXXXXXX950klpjcawuy4uj39ym43hs6cfsegq (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



Address Hunting using Specific Conditions

JBS Ransom Hack

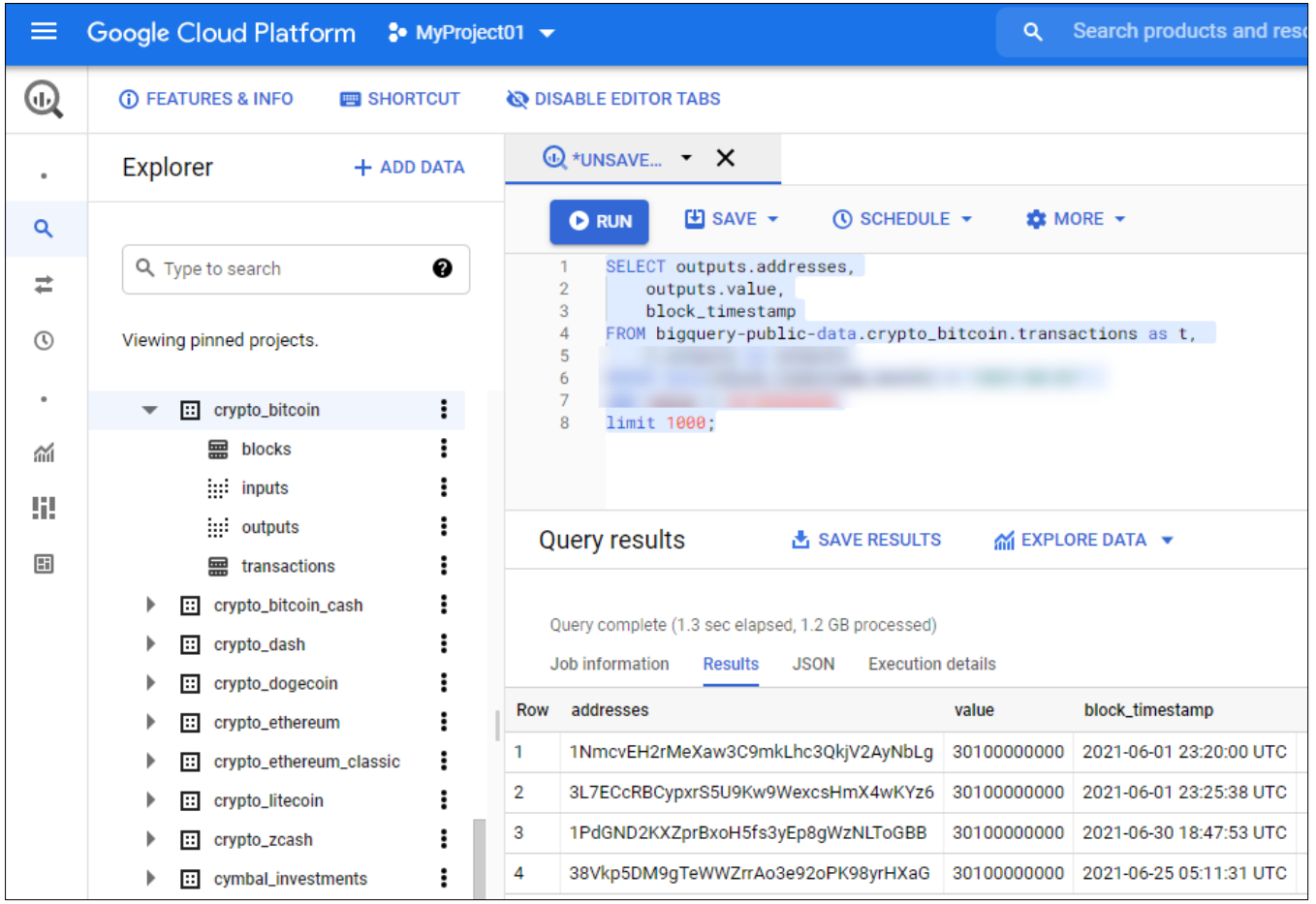
Meat giant JBS pays $11m in ransom to resolve cyber-attack

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.



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

#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

Source: bitquery.io

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: 32V6a7K46pSb1XQNGdrmdE2wjgndVfJPet
- Tx Hash: 185ee32a4d768b2ad739f907447884b0ae9b435e009d791a5ec67b8bfc235974

Let’s identify the attribution of the address!

bitinfocharts.com

Bitcoin Transaction 185ee32a4d768b2ad739f907447884b0ae9b435e009d791a5ec67b8bfc235974

Share:

block, address, transaction | Search

Block	582296
Time	2019-06-24 20:12:21
Size	387 (bytes)
Total Input	433 BTC
Total Output	432.99962058 BTC
Fees	0.00037942 BTC

prev tx	32V6a7K46pSb1XQNGdrmdE2wjgndVfJPet wallet: BetVIP	-433 BTC
	12n3s8MCqdZzPnTisYrXagbfw8pJg8y9BW	300 BTC
	bc1qpqttn46ndlm2e5ejurz3v33x79ku37v6m7nz0u wallet: 51934323	15 BTC
	bc1qmftdfx6xxkju36e8xuncfl6a967jqgp6uuza7l wallet: 51934323	15 BTC
	bc1q9seyqfwzt8zkuurqcz4ghpzge7ettz6x2vq75a wallet: 51934323	15 BTC
	bc1q9266jp27jwf2nzpszp4mgyraduynql4r0s7zcj wallet: 51934323	15 BTC
	bc1qu4rv5lm5mwhrusva2je8u7vsh0kdvzvw9n2r7e wallet: 51934323	15 BTC
	bc1qqk6fl03h2anhcncvfzs2c3uqvmllj4dreprk77 wallet: 51934323	15 BTC
	bc1qzk9l0t2zyjsz82dlxclwvyy0fqethpm4yy38xc wallet: 51934323	15 BTC
	bc1qsgz3ytwxpsgzukfrv89zkjwzgqwvttyrzv9u8n wallet: 51934323	15 BTC
	bc1q02jxxwnwdq859j2nhylw6fy8m9sa38gjtv03jr	12.99962058 BTC

Fee: 0.00037942 BTC

Source: bitinfocharts.com

Transaction sum: 432.99962058 BTC

whale-alert.io

api.whale-alert.io/v1/transaction/bitcoin/185ee32a4d768b2ad739f907447884b0ae9b435e009d791a5ec67b8bfc235974?api_key=Vf06G...


```
{
    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.

Source: whale-alert.io

clankapp.com

clankapp.com/bitcoin/address/32V6a7K46pSb1XQNGdrmdE2wjgndVfJPet

clank

Bitcoin > (coinbase) 32V6a7K46pSb1XQNGdrmdE2wjgndVfJPet

Top 100 | Richlist

Balance

$0.00

0.00 BTC

Total of transactions

5,031

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
$ 6,082,890 152.000 BTC	huobi 1KsFYJHLC1bSCRekPGzh...	→	coinbase 32V6a7K46pSb1XQNGdrm...	1 day ago 2021-07-30 02:47:57
$ 5,557,220 139.000 BTC	multiple addresses	→	coinbase 32V6a7K46pSb1XQNGdrm...	2 days ago 2021-07-29 01:00:24
$ 1,488,880 38.000 BTC	multiple addresses	→	coinbase 32V6a7K46pSb1XQNGdrm...	3 days ago 2021-07-28 16:52:15

Source: clankapp.com

walletexplorer.com

Wallet [00000014ea] (show transactions)

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

address	balance	incoming txs	last used in block
1FZe3YGmEgWfrg9VmRPJL5bKcRYavi7XHF	0.	1	194353
1GEpgGPBvc7zs9sp7npQ1cviBCLnsyyKqx	0.	1	194353
1J2AUr1PyKGoAjR6pjMFdc1tYJi9UVgw73	0.	1	194353
1JuMZ8jZdgZPn4Bs8q49mkZEJqfpy4msuH	0.	1	194353
1KS6ywkBEsf53aivGhuzESMXHvsnxFrom5	0.	1	194353
1DgtGU2PXi4iJQaHNbAcuGecjBGyJfJXC6	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.	e7f495e722ab47388051bcc19ec6371e2cb7d89952a29431ba80051d8ac7bf97
2012-07-06 06:33:36	+0.1	0.1	cc287a9790ab776da2e11250891e184e05b704535c2db65d2358213862712b41

Page 1 / 1 (total transactions: 2)

Source: walletexplorer.com

About 20,900,000 results (0.61 seconds)

Coinbase / Founded

June 20, 2012

coinbase

People also search for

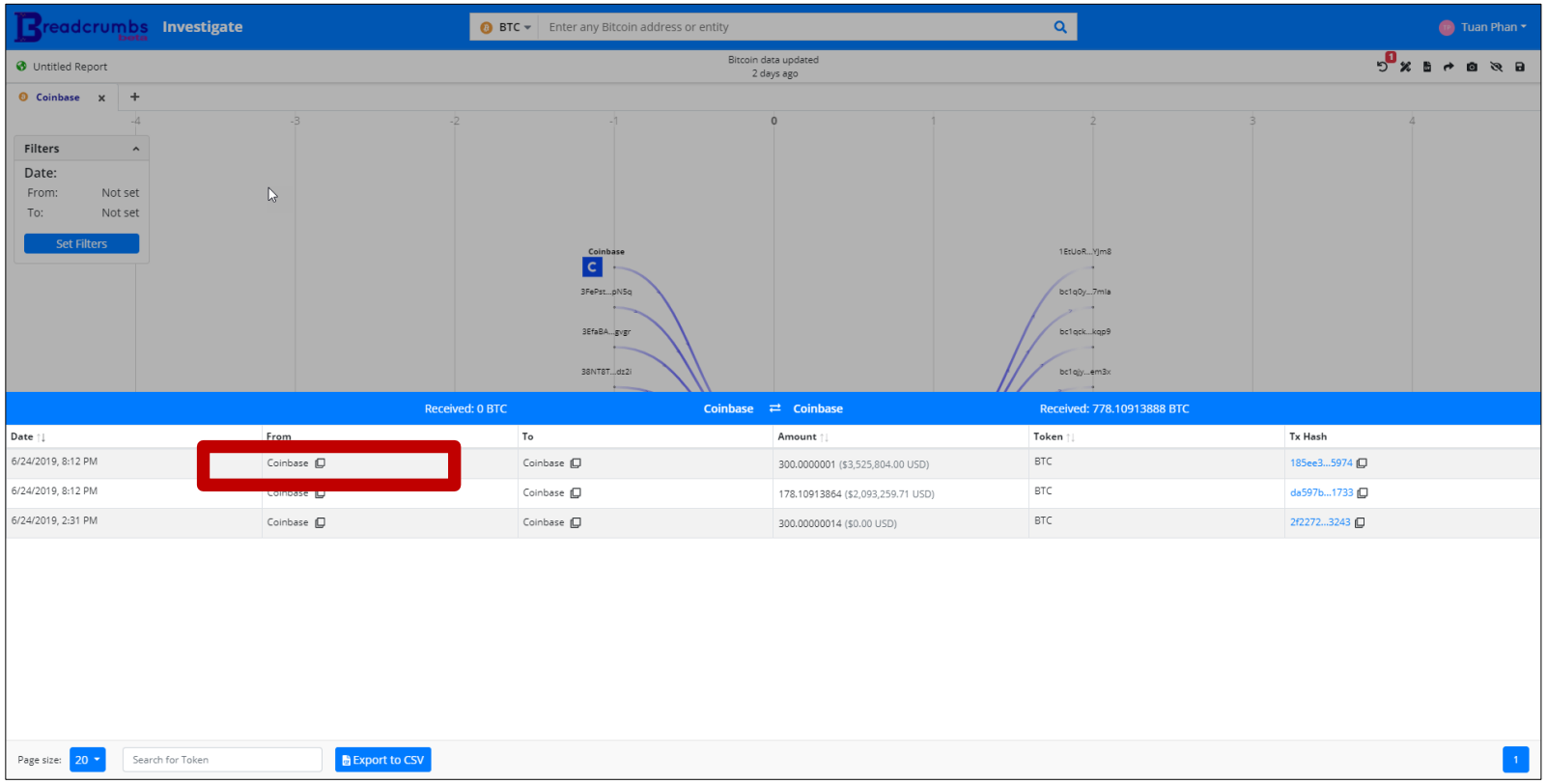
Binance
July 2017

Robinhood
April 18, 2013

Gemini
2014

Source: google.com

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)

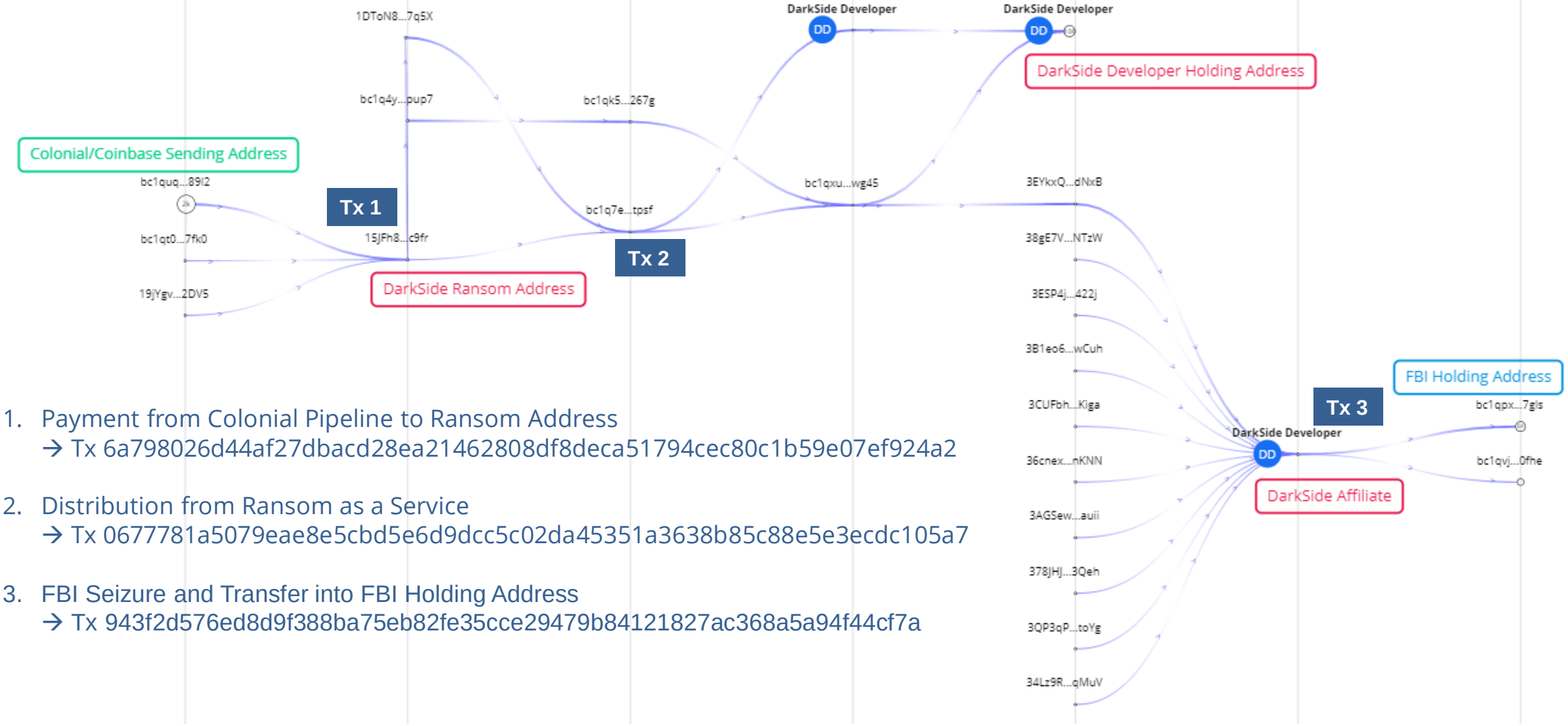
- Transaction hashes provides the provenance information recorded.
  - Authenticity
  - Integrity
  - Reliability
- For seizure action, specific transaction hash must be specified.

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

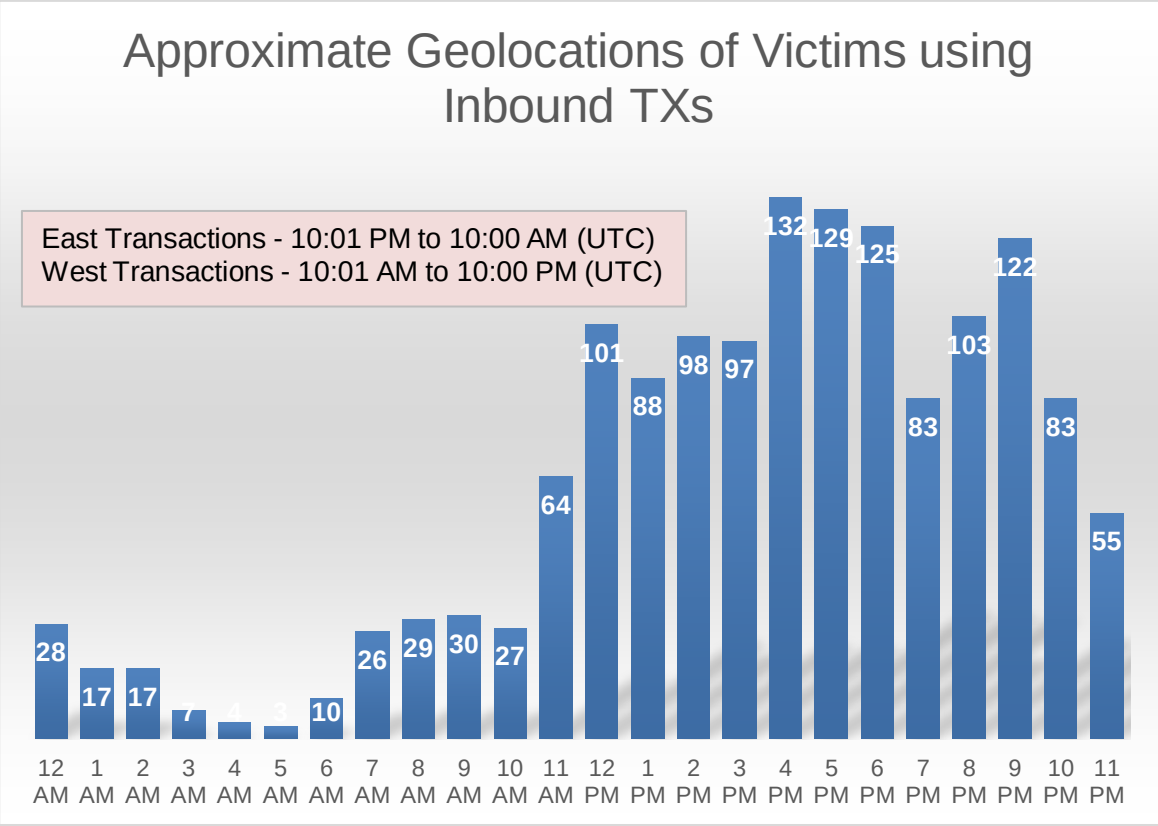
Special Topics

- 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

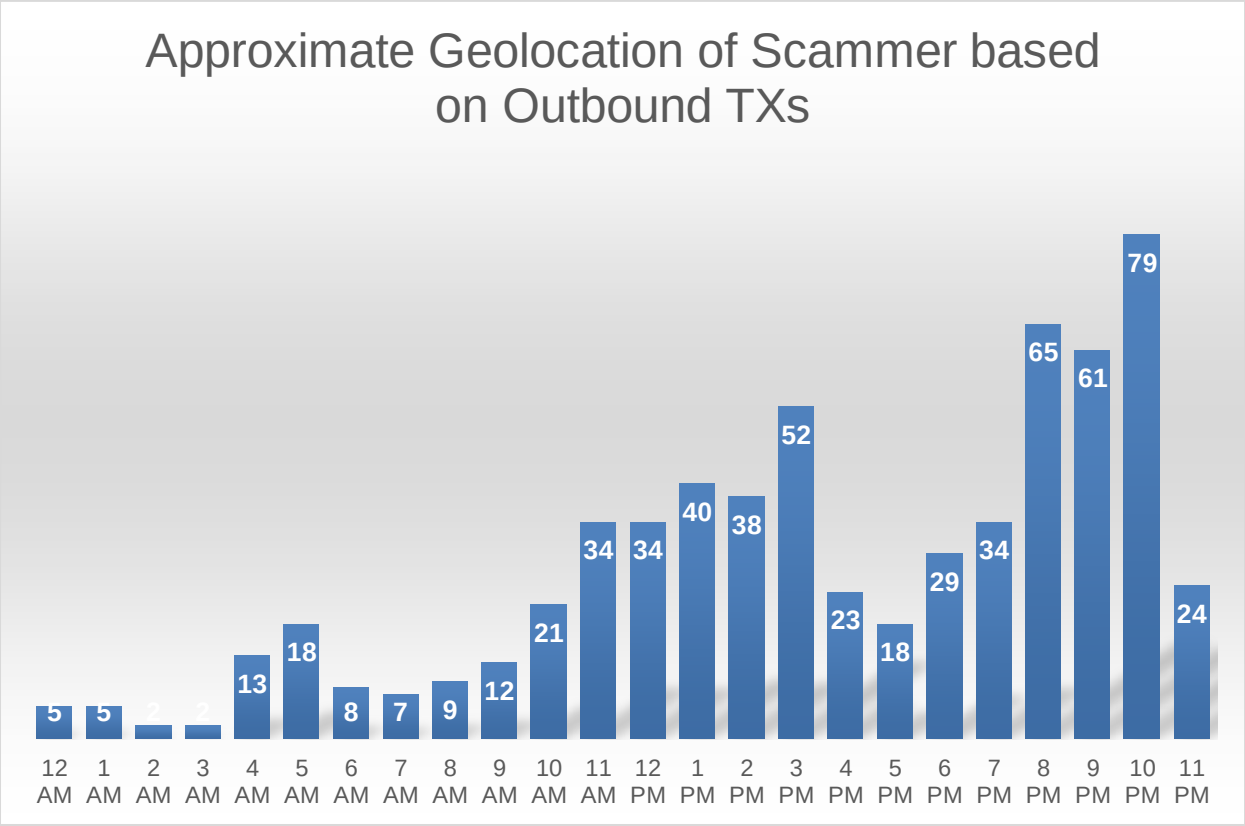
- Specific (Bitcoin) IP of transactions can also be collected using earliest broadcast method.

Geolocation using Transaction Timestamp

Tether Exchange Scam



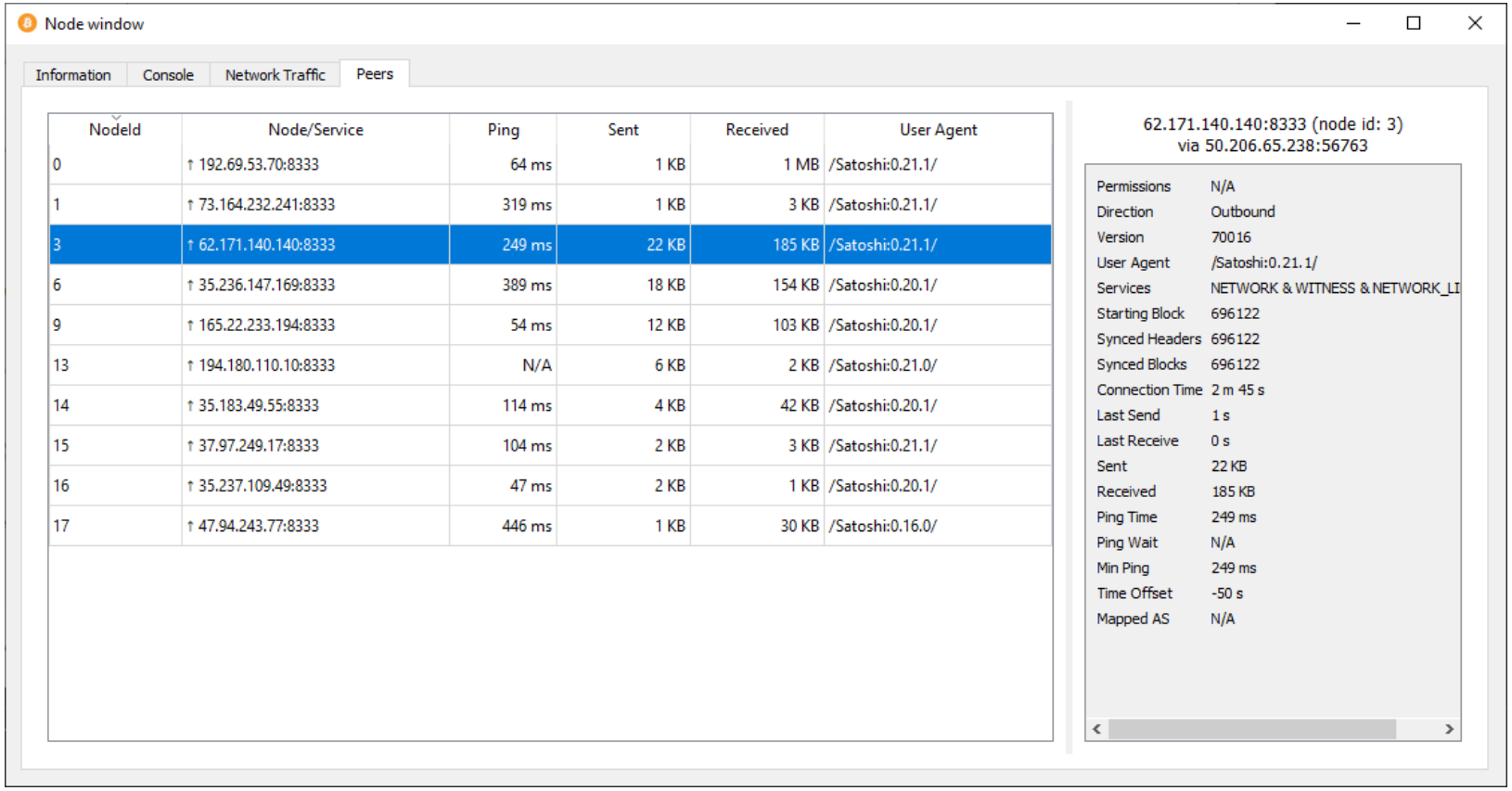
Most victims are from Western countries such as UK, Germany, and similar.



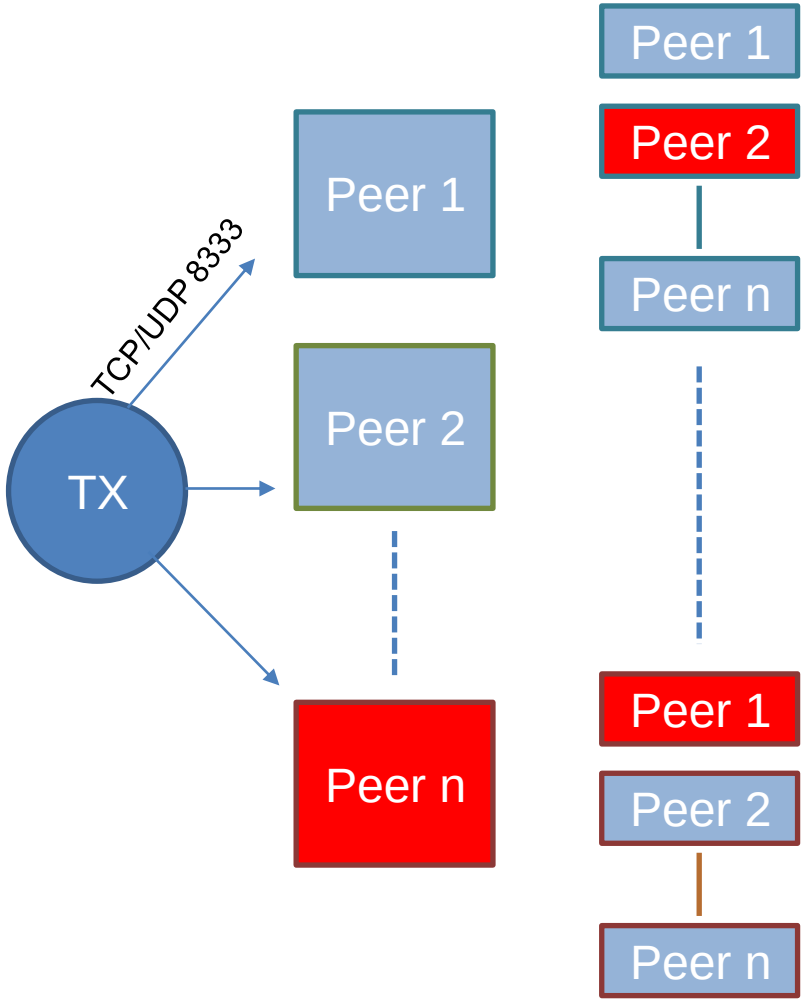
Likely to be based in Western countries as most transactions are between 10 AM and 10 PM.

Identifying the Earliest Broadcast of Specific TX

Propagation of TXs to Peers on Bitcoin



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/



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>/

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.

Viewer | Text


```
JSON
  inv_hash : "943f2d576ed8d9f388ba75eb82fe35cce29479b84121827ac368a5a94f44cf7a"
  stats
    std : 2428
    head
      0
        0 : "xywyvvvcs5pohots5lelilnigze5ittndtepmyerqzlshf4nom3pyfyd.onion:8333"
        1 : 1623087625504
      1
        0 : "in7r5ieo7ogkxbne.onion:8333"
        1 : 1623087626384
      2
        0 : "cncwik3tnd2ejm5z.onion:8333"
        1 : 1623087626423
      3
        0 : "rk4vbyca7xnn3top.onion:8333"
        1 : 1623087626560
      4
        0 : "pnd6ujrytfwabe4m.onion:8333"
        1 : 1623087626804
      5
        0 : "gkzo2hlkmdkwbj2v.onion:8333"
        1 : 1623087626888
      6
        0 : "52.15.186.116:48333"
        1 : 1623087626920
      7
        0 : "63.32.178.253:8333"
        1 : 1623087626931
      8
        0 : "[2002:d1b1:5615::d1b1:5615]:8333"
        1 : 1623087626934
      9
        0 : "54.185.108.174:8333"
        1 : 1623087626934
    min : 880
    max : 10118
    50% : 5494
    90% : 9077
    mean : 5723
```


Viewer | Text


```
JSON
  inv_hash : "280c5f96397b9502b99703842712b78fda84f1a0faabf826f683448082f46369"
  stats
    std : 1056
    head
      0
        0 : "rk4vbyca7xnn3top.onion:8333"
        1 : 1623088121619
      1
        0 : "xywyvvvcs5pohots5lelilnigze5ittndtepmyerqzlshf4nom3pyfyd.onion:8333"
        1 : 1623088122205
      2
        0 : "yzlai35raddd2kdjnukns7u5t4m4ngi5dfrlq72e6lqf2hp5dzkuszqd.onion:8333"
        1 : 1623088122345
      3
        0 : "v5i7np5tvgqkook2.onion:8333"
        1 : 1623088122352
      4
        0 : "6awaoeg6duhngrvd.onion:8333"
        1 : 1623088122510
      5
        0 : "ndgi74ath5c7j5d2.onion:8333"
        1 : 1623088122569
      6
        0 : "in7r5ieo7ogkxbne.onion:8333"
        1 : 1623088122667
      7
        0 : "hyw3lm5us7fnamyd.onion:8333"
        1 : 1623088122799
      8
        0 : "kgcarpwdts5y5xhu.onion:8333"
        1 : 1623088122896
      9
        0 : "gnwq5b3pvdiymn7d.onion:8333"
        1 : 1623088122931
    min : 586
    max : 5767
    50% : 3962
    90% : 5531
    mean : 4240
```


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

@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

LocalBitcoins

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 - verification of identity for KYC a AML
- Prone to market manipulation a 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

changelly

ShapeShift

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

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

Bcash

Cointral
Central Cash Coin

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

Deribit™

LedgerX

BitMEX

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?