Exhibit 'A'

CIPHERTRACE

Data Credibility in Cryptocurrency Investigations

The Black Box Approach

Black box analytics hinder investigations and impair testimony

UNVERIFIED SOURCES
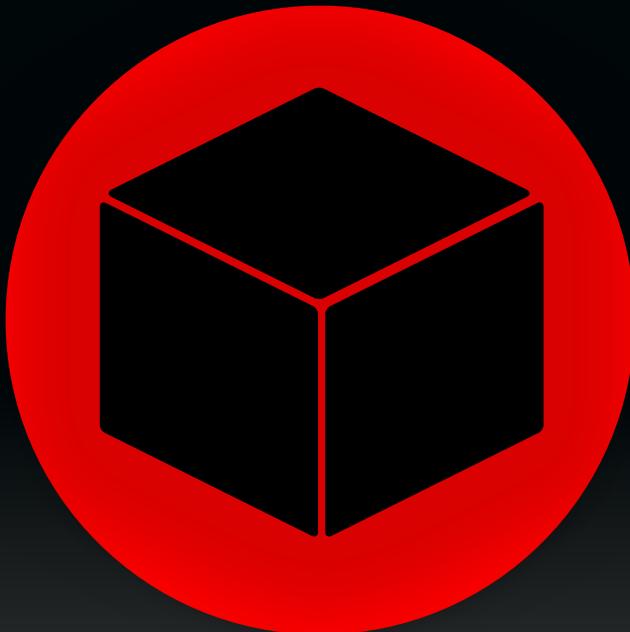
CANNOT BE USED IN A COURT OF LAW

CIPHERTRACE

How attribution data can be collected

CREDIBLE ANALYTICS

OTHER ANALYTICS

VERIFIED OPEN

Active Live Accounts
Dark Market / Deep Web
Full Blockchain Nodes

ACTIVE

Hunting and Targeting
Malware Analysis
Honey Pots

PRIVATE

Verified User Feedback
Private Threat Intelligence
APWG eCrime Exchange
Stolen Cryptocurrencies
Fraudulent ICOs
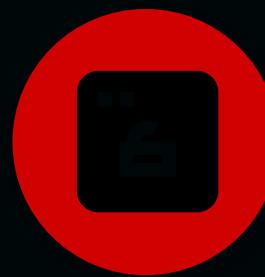
UNVERIFIED OPEN

Unverified databases and
open forums
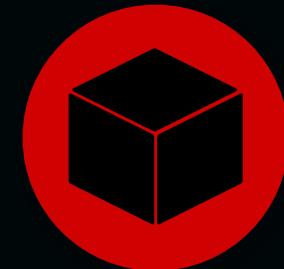
BLACK BOX

Potentially unauthorized
customer data, unverified
user feedback, clustering
errors and false positives

3

CIPHERTRACE

Importance of model validation

- Customers of a blockchain analytics provider may not know they are using a **Black Box** model.

- Model validation verifies the **accuracy** of the data enrichment and checks the **performance** of the model.

  - Providers should have well documented, auditable processes for attribution and clustering.

  - Providers should assess ongoing and historical attribution and clustering activity.

4

CIPHERTRACE

Clustering Approaches

CIPHERTRACE

SEPARATED CLUSTERS

PROS

✓ High fidelity

✓ True to blockchain

✓ Easily verify attribution

CONS

✗ Separate clusters won't group together visually

HYDRA MARKET

CLUSTER 1
- 1JRE……..
- 1pKR……..
- 17pM…….
  .

CLUSTER 2
- 32L9……..
- 3g7K……..
- 3VeX……..

CLUSTER 3
- bc1q4……..

SINGLE ENTITY CLUSTER

HYDRA MARKET

- 1JRE……..
- 1pKR……..
- 17pM……..
- 32L9……..
- 3c88……..
- 3VeX……..
- bc1q4…….
- …………….
- …………….
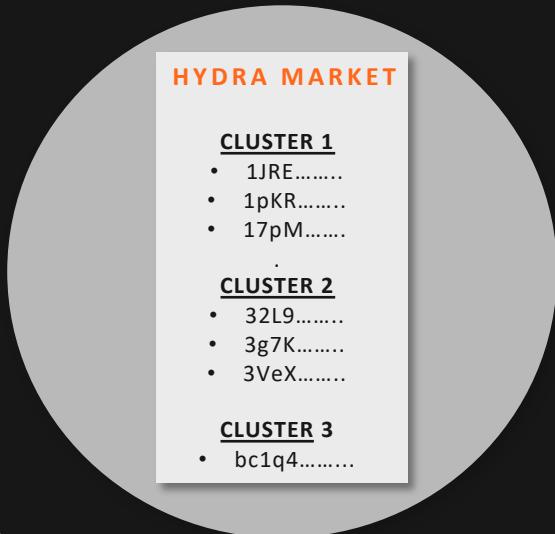
PROS

✓ Quick, high-level overview

CONS

✗ Not verifiable

✗ All data is lumped together

✗ Higher probability of false positives and errors

Separated Cluster Example: Al Qassam Brigades

3LhP8JYJ77cj2eVXBasY92Z6omTyRbUdbh

17QAWGVpFV4gZ25NQug46e5mBho4uDP6MD

Separated Cluster Example: Al Qassam Brigades

3LhP8JYJ77cj2eVXBasY92Z6omTyRbUdbh

17QAWGVpFV4gZ25NQug46e5mBho4uDP6MD

Case Study

Single Entity Tracing

A *Global exchange* was contacted by a blockchain analytics firm (utilizing wallet-based tracing tools) who informed them that they had a customer send a very small BTC donation to al Qassam Brigades.

Global exchange approached CipherTrace to verify the trace:

*recreated trace view

Global exchange → 0.1 BTC → Self-custody address → 0.1 BTC → Entity #1 → 6.31 BTC → Entity #2 → 0.1 BTC → Self-custody address → 0.1 BTC → Al Qassam Brigades

CIPHERTRACE

Case Study
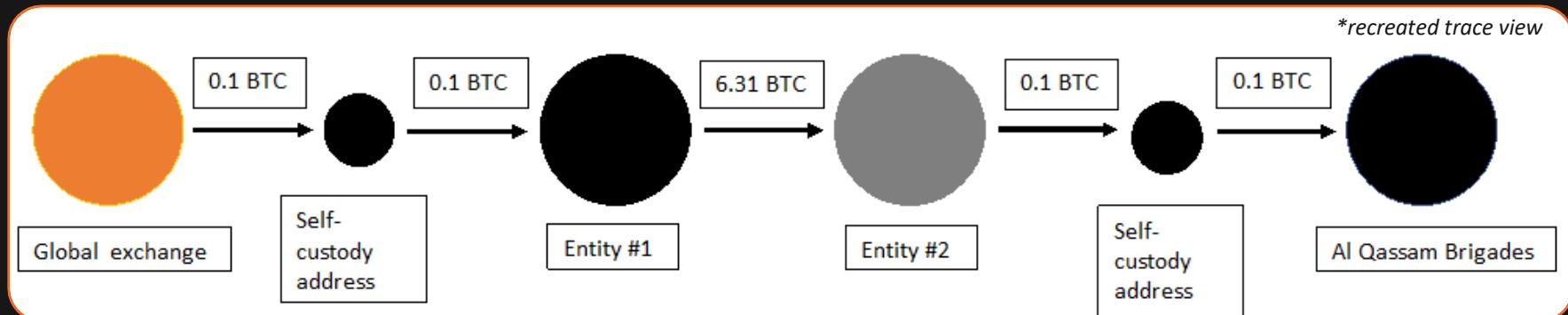
Single Entity Tracing

What the on-chain trace actually looks like.
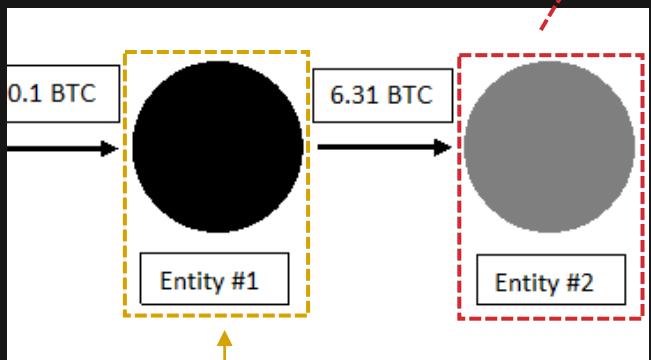
CIPHERTRACE

Case Study

Single Entity Tracing

Wasabi CoinJoin

ADDRESS: BITCOIN (BTC)
bc1qr

OWNER **WASABICOINJOIN**
TYPE **MIXER**
CLUSTER

RISK **10**

CURRENT BALANCE
0.00000000 BTC

RECEIVED
0.20994056 BTC
1 Transactions

SENT
0.20994056 BTC
1 Transactions

FILTER TRANSACTION
ALL ADDRESSES

DATE RANGE FILTER
1/3/2009 - 8/25/2022

Viewing page

RISK	DATE/TIME ^	TOTAL AMT ▼	ADDR AMT ▼	TRANSACTION ID	RECEIVED	SENT
	JUN 4, 2021 04:54:00 AM	25.12324428	0.20994056	75c		
10			0.77232184			bc1qx
9			0.19278732			bc1qx
9			0.09654878			bc1qc
9			0.08452767			bc1qq
9			0.19308046			bc1qk
9			0.09654878			bc1q4
9			0.09654878			bc1qh
10						bc1ql2

CIPHERTRACE

Case Study

Artificial Clustering w/ Cluster Based Tracing

CipherTrace was asked to verify the following trace:

recreated trace view

Self-custody address

9.17 BTC

Source of theft
Un-hosted address

1PAaf
Wallet 1

472.76 BTC

1Bade
Wallet 2
(OTC desk collection address)

307.83 BTC

Client:
VASP - OTC Desk
Funds Freeze Request

CIPHERTRACE
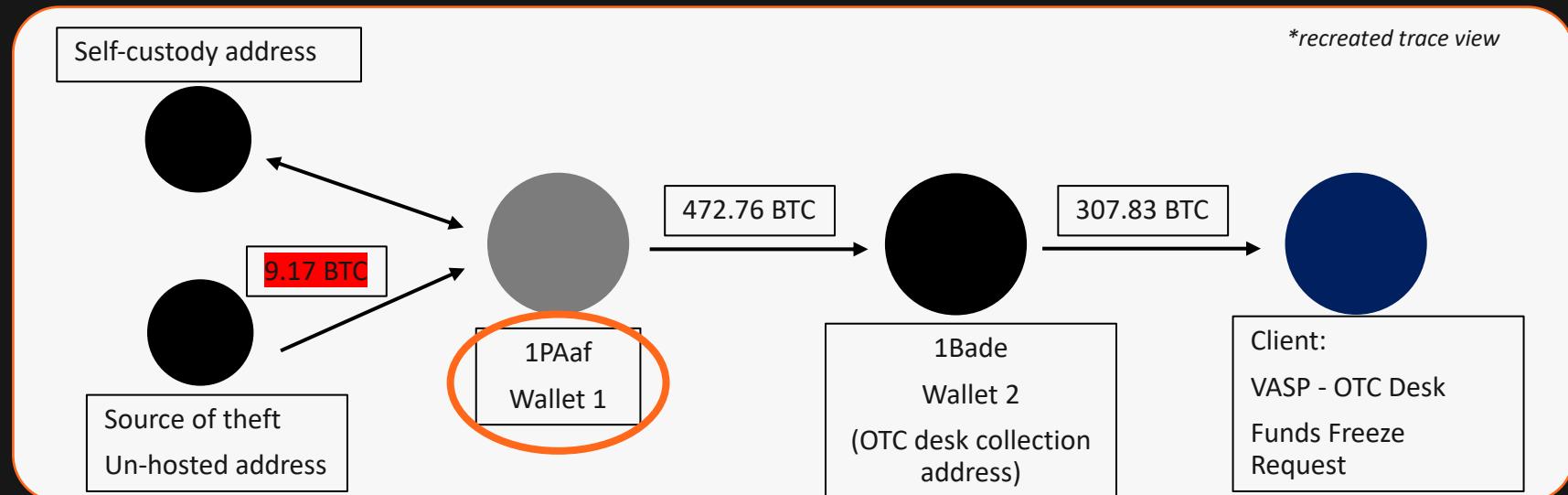
Destination Output 1PAaf

Address   1PAafXXXXXXXXXXXXXXXXXXXXXXXXX

Transactions   3

Total Received   0.79950000 BTC

Total Sent   0.79950000 BTC

Final Balance 0.00000000 BTC

1PAafk	0.40040000 BTC 🌐➡️	17PgF	0.00391625 BTC 🔴
1PAafk	0.39910000 BTC 🌐	1H2M3	1.19500000 BTC 🔴
1A9YK z	0.39960000 BTC 🌐		
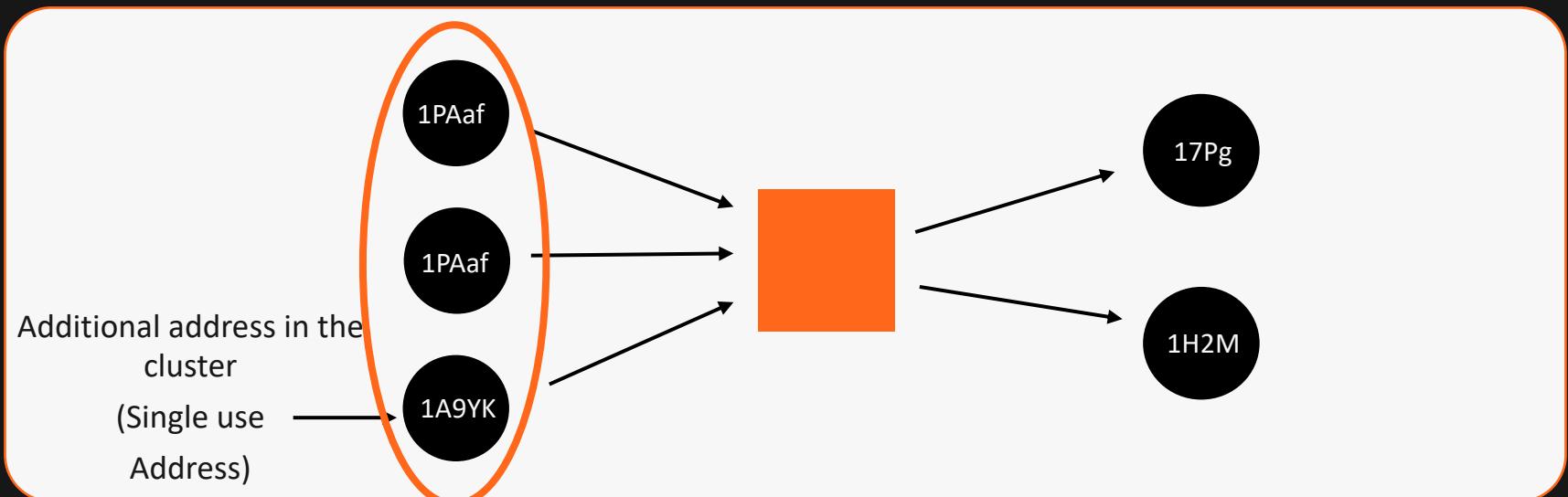
Artificial Clustering w/ Cluster Based Tracing

9.17 BTC Transaction

5 Exchanges

2 Services

CIPHERTRACE

Case Study

Artificial Clustering w/ Cluster Based Tracing

19 hops

9.17 BTC Transaction

CipherTrace stopping point.

VASP client's Deposit Peel-chain

Peel-chain consolidates with other high-volume deposits.

CIPHERTRACE
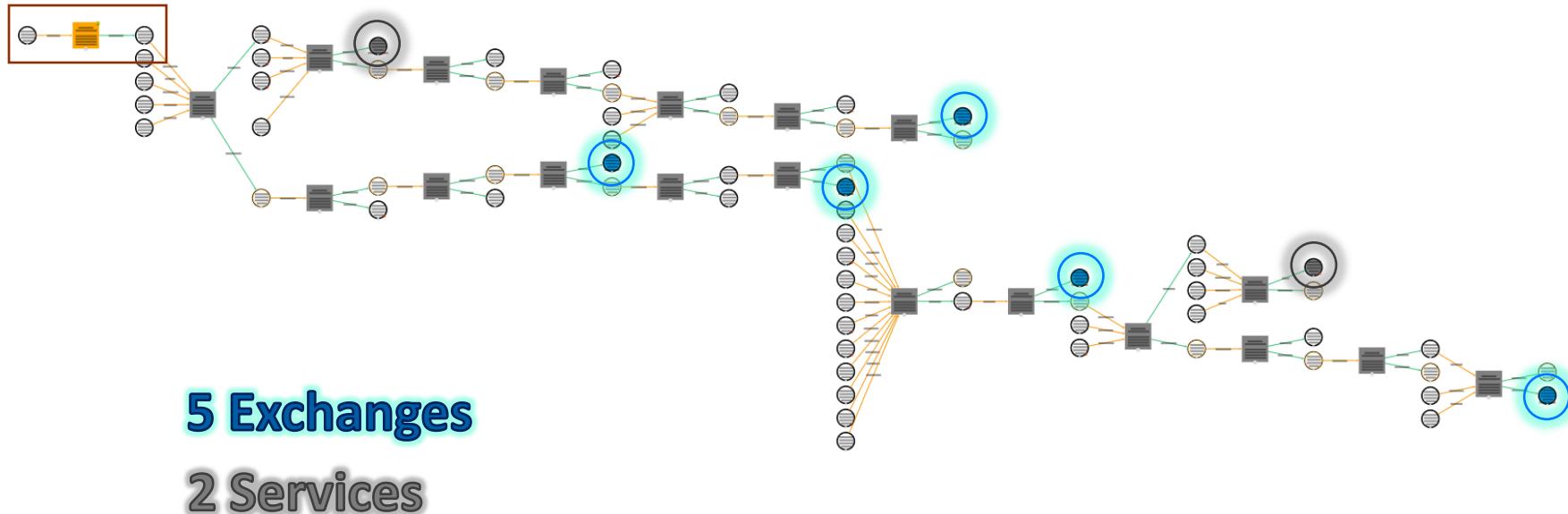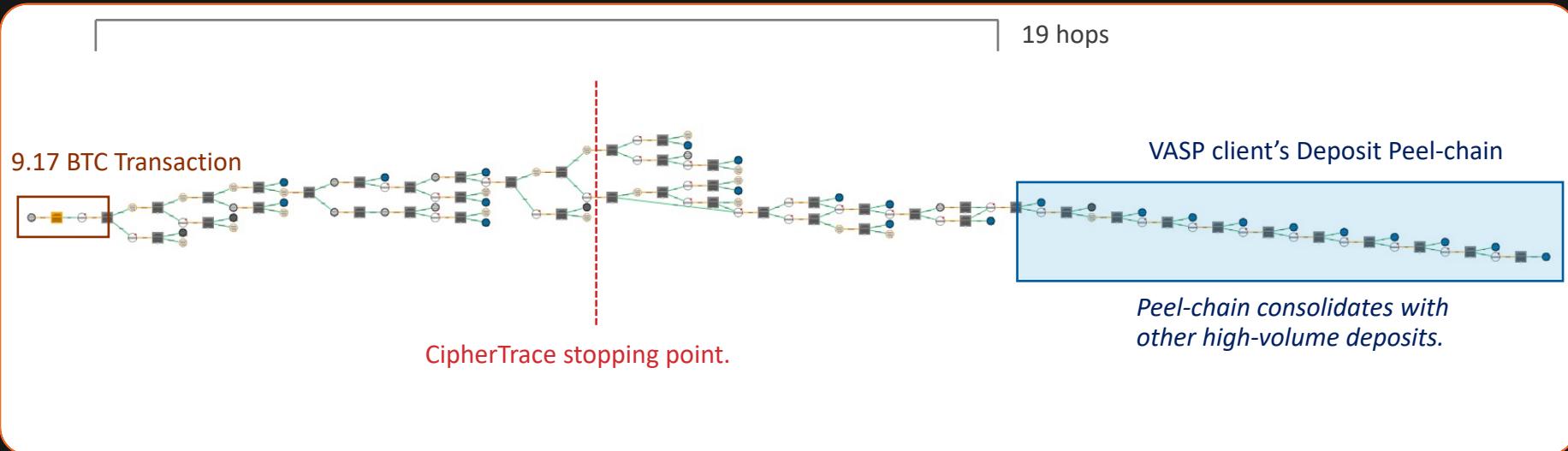
Clustering False Positives

- There are known false positives that exist for clustering heuristics, which require investigators to look at and rely on other data points to confirm clustering.

- Important to not just cluster addresses and never look back at them

- Most common example of technique used to break clustering heuristics is coinjoins.

These addresses would traditionally cluster together, but shouldn't if in a coinjoin

2 BTC — ALICE

3 BTC — BOB

1 BTC — EVE

TX

.05 BTC
Transaction Fee

1 BTC

1 BTC

4 BTC

CIPHERTRACE