# INVESTIGATIVE CONSIDERATIONS

# EXERCISE

- Discussion - Outline the following in respect of your agency and it's position on virtual assets:
  - Are virtual assets seen as a significant threat? If so what rationale has been provided for this.
  - What legislation can be utilised to assist with investigations involving virtual assets?
  - What framework/s has been developed to capture evidence relating to virtual assets?
  - What training is provided in respect of virtual assets?
  - What would make your agency more efficient in investigating matters involving virtual assets?
  - How well informed is the criminal justice system as a whole?

# VIRTUAL ASSET INVESTIGATIONS

- When starting an investigation into money laundering involving virtual assets it is important to consider the following:
  - There will potentially be a lot of data to analyse
  - There may be multiple interpretations of the data
  - Misinterpretation of data can lead to collateral intrusion on innocent third parties
  - The technical nature of some data will be difficult to explain
  - Data may be held in jurisdictions based in any part of the world.

- The key takeaways are:
  - You will need to organise your investigation from the get go. Audit trails will be very important.
  - You need to accept that there could be alternative explanations for the patterns shown in the data and be transparent in regards to this.
  - Any approach to a crypto asset entity for data needs to be justified and collateral intrusion considered.

- Repeatedly re-visiting blockchain data for investigative purposes could be seen as surveillance.
- Data held in foreign jurisdictions may be provided as intelligence with no legal oversight. Obtaining that information for evidential purposes will likely require a legal order (MLAT/ILOR etc.).
- "*Work smarter not harder*", carefully consider if virtual asset enquiries will progress your investigation most efficiently. Other evidence may do a much better job and be much easier to work with.
- If you are to use any data as evidence there will be a challenge in getting other aspects of the criminal justice system to understand it's significance. This can be a double edged sword as a lack of understanding could lead to miscarriages of justice. As such it is important to make sure every effort is made to corroborate data through other means and all parties in the criminal justice process have opportunity to understand the evidence.

# What is Blockchain Analysis?

- The days of believing that Bitcoin is completely anonymous are long gone. Over the last few years significant research has been done on tracing Bitcoin transactions and attributing addresses to entities. The over arching term for this process is called blockchain analysis.
- Essentially this is the process of **analysing transaction data on the blockchain using a block explorer**. On transparent crypto asset protocols such as Bitcoin, **block explorers facilitate searching and examining every transaction recorded on the blockchain**. For Bitcoin this extends back all the way to the genesis block in 2009.
- The **transaction data can be used to identify insights into criminal activity such as patterns of behaviour, clustering of addresses and points of friction with the traditional financial world**. There is a caveat though, **blockchain analysis makes assumptions based on common heuristics which do not always hold up to be true**. It is important to have a good grasp of the basics in order to make good judgements when utilising the results of deploying the tactic.

The methodology we will focus on is relevant to Bitcoin and protocols which copy it's UTXO model. Bitcoin's significant adoption and deep liquidity still makes it the most practical cryptocurrency for money laundering. As a result the majority of criminality involving cryptocurrencies will utilise Bitcoin.

There is however a growing number of cryptocurrencies which have nuances of their own in relation to analysis. Further to this there are blockchain and distributed ledger technologies starting to be deployed in a range of business sectors.

It is important to note that criminality has always been at the forefront of utilising new technology, as such there will be money laundering methodologies utilising other assets and protocols. Part of your challenge as investigators is recognising the evolution of criminality and finding a means of keeping pace.

- This is no mean feat and investigators across the globe struggle with this. Unfortunately there will never be a training course or session which sufficiently covers this subject. The onus is on you to utilise professional development opportunities and networking to take on the challenge. From my perspective I certainly worry about not being good enough and try to use this to motivate me into working harder. The need to keep learning and developing is something I imagine all of the instructors would echo.

- My point is that the following input and any others received as part of this course, should be seen as just one aspect of an ongoing professional development journey. Don't despair if the detail has been a bit too quick or not met your learning styles, there is still plenty to take away and lots of contacts to network with.

# Heuristics

- **"Clustering addresses"** refers to the process of attributing numerous addresses to the same wallet/controlling entity through the use of transaction behaviour heuristics.

- There are a number of factors which go into these heuristics. We will cover some of the well known ones in the following slide. It is important to note however that none of the heuristics are definite. They can be wrong and as investigators it is necessary to corroborate the results.

- Cryptocurrencies focused on principles of self sovereignty recognise blockchain analysis as an attack on the network. **Small minorities within these communities are working to break the heuristics used and minimise the ability to undermine privacy within the protocol**.

- The key point here is that the methods being used to provide Blockchain Forensic Tools is likely to evolve in line with efforts to break the heuristics. It could become more difficult to identify how results are being provided and this makes it important to keep informed on the subject.

## Heuristic 1 – Common Input Ownership

Assumption: All inputs in a transaction belong to the same entity as they reside in the same wallet.

- Vast majority of bitcoin transactions are simple in nature. Very few collaborative transactions.
- As a result one wallet controlled by one entity will have provided all of the transaction inputs to send funds.

## Heuristic 2 – Change address detection:

- Change amounts are linked to addresses never previously seen in the blockchain.
- If an output address is the same as an input address it is the change.
- Wallet fingerprinting can be used to detect change outputs because a change output is the one spent with the same wallet fingerprint.
- Round numbers as an output are payments not change.
- If the values of the inputs are more than one of the outputs but less than another, the lower figure output is change (Unnecessary input heuristic) e.g.

| Inputs | Outputs | Assumption |
|---|---|---|
| 1BTC | 3.5BTC → | Payment |
| 2BTC | 0.5BTC → | Change |
| 1BTC | | |

Assumptions:

- **If an output address has been reused it is very likely to be a payment output**, not a change output. This is because change addresses are created automatically by wallet software but payment addresses are manually sent between humans.

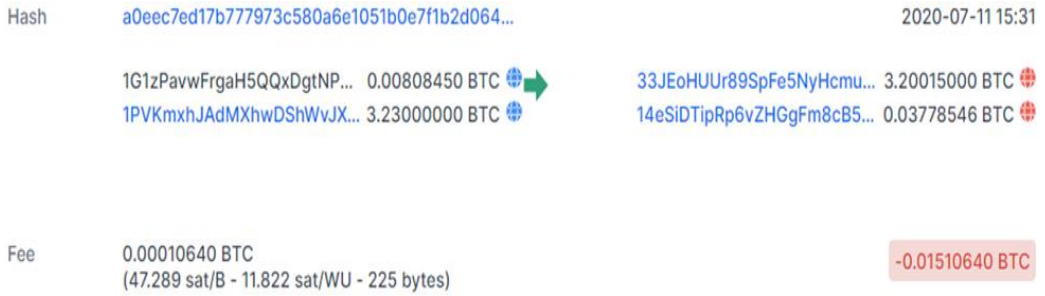
- Entities utilise wallet defaults for coin selection and fee payments.

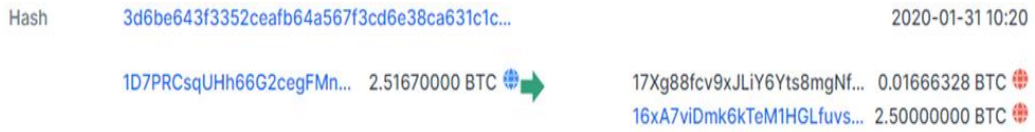
- **Many payment amounts are round numbers**, for example 1 BTC or 0.1 BTC. The leftover change amount would then be a non-round number (e.g. 1.78213974 BTC). This potentially useful for finding the change address. The amount may be a round number in another currency. The amount 2.24159873 BTC isn't round in bitcoin but when converted to USD it may be close to an exact dollar value.

# Heuristic examples


**Common input heuristic**

**Change heuristic:** Outputs are different script types.




**Change heuristic:** The address 16xA7 was active prior to this transaction. The address 17Xg88 was first active as part of this transaction. Round payment made to 16xA7 address

# Private intelligence

Further to these heuristics Blockchain Forensic Tools will **utilise industry intelligence and covert surveillance tactics to attribute entities to addresses and build clusters**. This will mean it is often **opaque as to how an identification or cluster has been developed**.

It is possible to try and find connections. You can manually check for the heuristics and carry out open source research. This may however become unpractical (if significant amounts of data) or turn out to be inconclusive. In these instances it would be worth noting down the efforts made and the negative result. Such process will at least show efforts have been made to understand the intelligence and quantify it's origins.

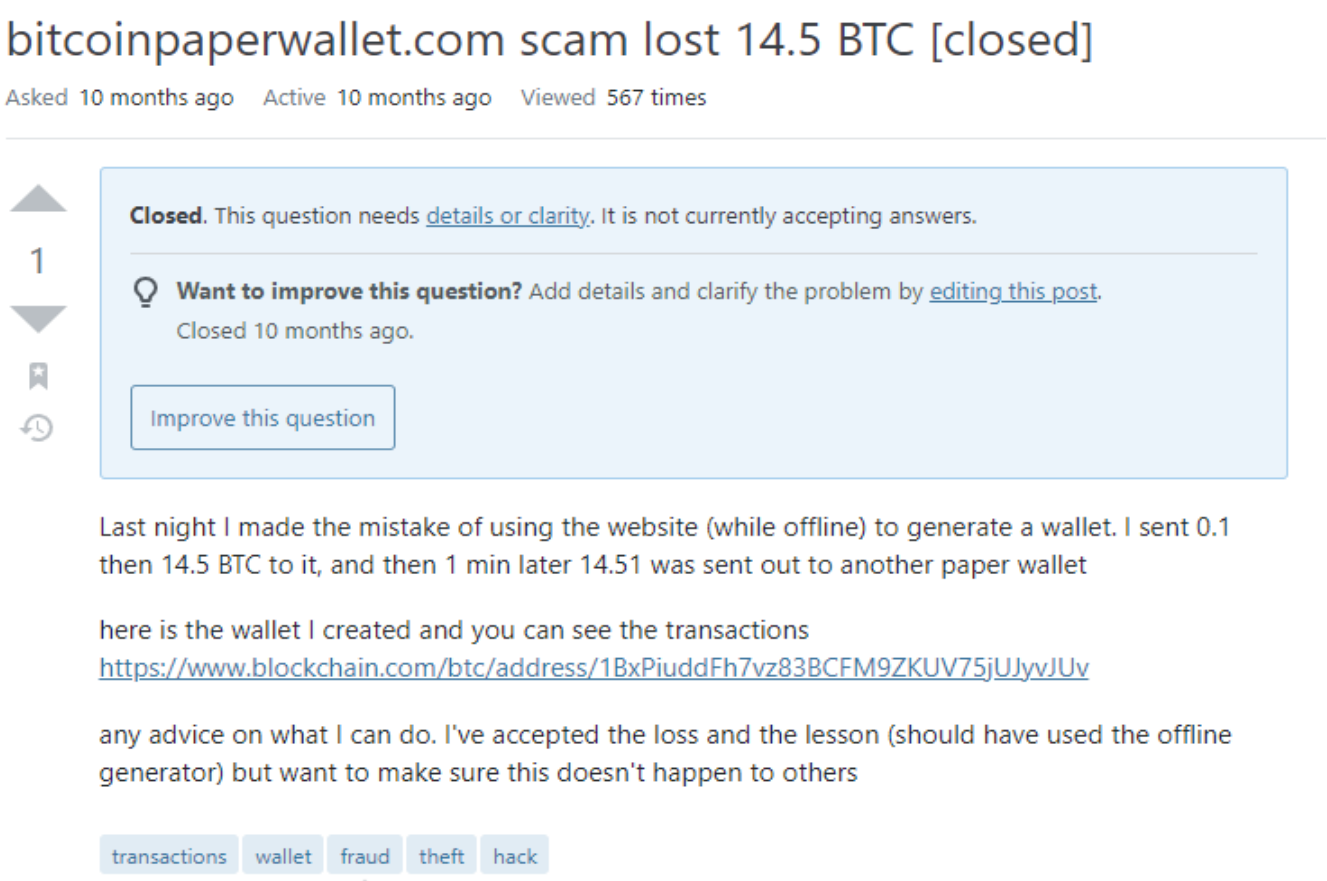
# DEVELOPING AN INVESTIGATION STRATEGY

- "Investigation strategies are dynamic in nature, because the active and conscious opposition from our 'antagonist' changes steadily and continuously our plans" (Europol, 2017)
- Apologies if this is basic, in my experience this is still missed on occasion and often weak in it's content.
- To reflect this we need to plan strategies carefully being mindful to review and update them regularly as new information comes to light.
- Thought also needs to be given to the parameters being applied to investigation strategies. Whatever data we look at as part of the investigation is potentially disclosable in a court situation. For this reason it is vital to carefully consider what is worth looking at and what isn't. Volumes of data can quickly build up if parameters are not set early on in a strategy.

- **Blockchain analysis:**
  - Outline objectives, what parameters have been set and why?
  - What tools will be used? What process will be used to corroborate relevant data?
  - How will data be captured and evidenced? what legalities are involved in completing the process?
  - Risk assessment on suitable tools.
- **Data analysis:**
  - What analysis needs to be carried out on any data captured? Are any other resources required to assist with this?
  - What tools will be used to achieve this? how will data be stored?
- **Hypotheses:**
  - Is there a hypothesis on the circumstances in question or is it too early in the investigation to do so?
  - Have alternative interpretations been considered? Has the hypothesis been based on a gap or conflict in the evidence?
  - How is the process impacted by hypotheses? e.g. is the process aimed at locating specific material to test a specific hypothesis

- At the end of this we will be using the results to outline a new strategy reflecting the new evidence/intelligence gathered.

# Practical



## bitcoinpaperwallet.com scam lost 14.5 BTC [closed]

Asked 10 months ago  Active 10 months ago  Viewed 567 times

1

**Closed**. This question needs details or clarity. It is not currently accepting answers.

**Want to improve this question?** Add details and clarify the problem by editing this post.
Closed 10 months ago.

Improve this question

Last night I made the mistake of using the website (while offline) to generate a wallet. I sent 0.1 then 14.5 BTC to it, and then 1 min later 14.51 was sent out to another paper wallet

here is the wallet I created and you can see the transactions
https://www.blockchain.com/btc/address/1BxPiuddFh7vz83BCFM9ZKUV75jUJyvJUv

any advice on what I can do. I've accepted the loss and the lesson (should have used the offline generator) but want to make sure this doesn't happen to others

transactions  wallet  fraud  theft  hack

1. www.blockchain.com
2. https://oxt.me/
3. https://explorer.bitquery.io/
4. https://blockchair.com/
5. https://www.bitcoinabuse.com/
6. https://www.bitcoinwhoswho.com/

https://www.blockchain.com/btc/address/1BxPiuddFh7vz83BCFM9ZKUV75jUJyvJUv

# Blockchain analysis example

- The following example will demonstrate the interface of Chainalysis (a paid for blockchain analysis tool).
- An example graph will be drawn out using the tool to highlight the flow of funds linked to a theft.
- This will help visualise some of the opportunities available to investigators when using blockchain analysis.

# PROCESS FOR CAPTURING DIGITAL EVIDENCE

Blockchain analysis can be interpreted as open source research and we will be capturing digital evidence when we find relevant information. To help manage the volume of data, clearly identify the relevant information and make all of it accessible for disclosure it is vital to have a transparent, auditable and systematic process for recording the investigation.

Conducting enquiries in line with any process adopted will allow an investigator to demonstrate how they obtained their results. This allows for peer review and improves the quality of evidence available. In turn this should lead to better criminal justice outcomes as any issues with evidence can be identified at an early point.

Research and testing should be carried out before settling on such a process. In the UK there is no set process shared by law enforcement agencies, instead there are a number of principles which a process for capturing digital evidence should adhere to.

# THE PRINCIPLES OF DIGITAL EVIDENCE

In the UK digital investigation processes are based around the four principles detailed below:

- Principle 1: No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court.
- Principle 2: In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions.
- Principle 3: An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
- Principle 4: The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

The process can be automated in software or it can be manually completed. (Show example)

# SUMMARY

- Planning an investigation strategy is an important part of effectively investigating such offences. As the saying goes fail to prepare, prepare to fail!
- This exercise shows how blockchain analysis is not a simple subject. There is a lot of nuance and it is not a quick enquiry. This is why it is important to have a process that allows you to revisit information and spend time analysing it. The investigation strategy also needs to recognise this and seek to explore every option available to progress the case.
- It also shows how quickly you could get lost as analysing thousands of transactions is not easy! This is why parameters are important. Also identifying technology which can help with analysis is key to getting the best evidence out of such enquiries.
- There are positives in completing blockchain analysis if it can be managed effectively. It can help with identifying significant evidence for money laundering investigations. We can tell how much has gone to an account, how regular activity has been, we can use dates/times to compare against other relevant information e.g. times of offence or bank statements.