An Analysis of the MTI Crypto Investment Scam: User Case

Johnny Botha[1], Thor Pederson[2] and Louise Leenen[3]
[1]Council for Scientific and Industrial Research, Pretoria, South-Africa
[2]TCG Forensics, Cape Town, South-Africa
[3]University of Western Cape and CAIR, Cape Town, South-Africa

[1]jbotha1@csir.co.za
[2]thor@tcgforensics.co.za
[3]lleenen@uwc.ac.za

Abstract: Since the start of the Covid-19 pandemic, blockchain and cryptocurrency adoption has increased significantly. The adoption rate of blockchain-based technologies has surpassed the Internet adoption rate in the 90s and early 2000s. As this industry has grown significantly, so too has the instances of crypto scams. Numerous cryptocurrency scams exist to exploit users. The generally limited understanding of how cryptocurrencies operate has increased the possible number of scams, relying on people's misplaced sense of trust and desire for making money quickly and easily. As such, investment scams have also been growing in popularity. Mirror Trading International (MTI) has been named South Africa's biggest crypto scam in 2020, resulting in losses of $1.7 billion. It is also one of the largest reported international crypto investment scams. This paper focuses on a specific aspect of the MTI scam; an analysis on the fund movements on the blockchain from the perpetrators and members who benefited the most from the scam. The authors used various Open-Source Intelligence (OSINT) tools, alongside QLUE, as well as news articles and blockchain explorers. These tools and techniques are used to follow the money-trial on the blockchain, in search of possible mistakes made by the perpetrator. This could include instances where some personal information might have been leaked. With such disclosed personal information, OSINT tools and investigative techniques can be used to identify the criminals. Due to the CEO of MTI having been arrested, and the case currently being dealt with in the court of law in South Africa, this paper also presents investigative processes that could be followed. Thus, the focus of this paper is to follow the money and consequently propose a process for an investigator to investigate crypto crimes and scams on the blockchain. As the adoption of blockchain technologies continues to increase at unprecedented rates, it is imperative to produce investigative toolkits and use cases to help reduce time spent trying to catch bad actors within the generally anonymous realm of cryptocurrencies.

Keywords: Blockchain, Crypto scams, Crypto crime, Investigation, MTI, Process.

1. Introduction

Cryptocurrencies, Non-fungible tokens (NFTs), Decentralised Finance (DeFi) and smart contracts are all terms associated with blockchain technology. This technology has been growing at a rapid pace and provides unlimited applications. Some argue that Bitcoin gives power back to the people. However, the popularity of cryptocurrencies (crypto) has attracted the attention of many scammers and fraudsters. Undoubtedly, the rise of cryptocurrency has contributed to the immense increase in crime rates. Illicit transactions in cryptocurrency have reached a staggering $14-billion in 2021, an 80% increase from 2020 - this constitutes a new record (Sigalos, 2022) (Chainalysis, 2021). Scammers have always been around, but some of the characteristics of crypto are very appealing to them. Crypto has no middleman as in the case with banks. Instead, direct transactions occur between two individuals and transfers are much faster than traditional finance systems. When crypto is used on exchanges, the exchange can be seen as the middleman. Although many exchanges are still highly unregulated, they continue to act as the avenue to get crypto to fiat and vice versa. Pseudo names are being used on unregulated exchanges instead of actual personal details. It is difficult to trace crypto transactions and the space is relatively unregulated (Stylianou, 2022). Due to increasing regulations on crypto exchanges, some exchanges are gathering good *Know Your Customer* (KYC) information, others not at all (Lomas, 2023).

The Covid-19 pandemic brought difficult times with job losses and salary cuts. People became desperate to invest in alternative methods and crypto seemed like the perfect solution with the consequence that scammers took advantage of this opportunity (Xia, et al., 2020). Investigating and exploring cryptocurrency transactions remain intractably hard due to its pseudonymous nature and with every cryptocurrency having its own protocol and blockchain (Social Links, 2022).

Cryptocurrencies have become a popular target for criminals, and due to the nature of its design, criminals feel that they can commit crimes anonymously. However, cryptocurrencies are based on a public blockchain and visible to anyone. The flow of illicit transactions could be traced and investigated via advanced techniques with the goal of finding the destination cryptocurrency address that contains the stolen currencies. The next step as an investigator will be to unmask the owner of the address by combining Open-Source Intelligence (OSINT) and

KYC data collected from cryptocurrency exchanges. The investigator will then connect with law enforcement to have subpoenas issued in an attempt to seize or recover the stolen funds (Connors, 2022)

Some of the methods used by criminals to perform anonymous transactions on the blockchain are mixers or tumblers. These services combine cryptocurrencies of various users and send the crypto to another wallet. The investigator can then see that funds have been sent to the mixer and have been received by another person, but it breaks the direct connection between two individuals involved in the transaction. Criminals also make use of nested and unregulated exchanges that require no KYC and are not subject to Anti Money Laundering (AML) requirements. Criminals will often make use of privacy coins that are not tracable at all, making it almost impossible for investigators to trace the funds. Further more, Peer-to-Peer (P2P) decentralised crypto networks are being used, which also do not require KYC from customers. NFTs are often commonly used for money laundering. DeFi is the latest trend in the crypto space that has increased in popularity, and criminals have made use of this opportunity to send funds from illicit wallets (Stylianou, 2022).

Investors need to take all these methods into account when trying to connect the dots and follow the money. This paper analyses a specific, selected case on the Mirror Trading International (MTI) Platform. The case was selected from the website MTI-Leaks (MTI-Leaks, 2022). MTI-Leaks issued several publications with data on the founders of the scam as well as members who benefitted the most from the scam. In collaboration with TCG Forensic, a cyber-crime and digital forensics company based in South Africa, an initial process is proposed (section 3) on how certain crypto crimes can be investigated. This process is followed in section 4 where the case is analysed and investigated and concluded in section 5. Jeff Lomas, a detective and digital forensics examiner at the USA Las Vegas Metropolitan Police Department, kindly performed a review of the authors' investigation, and gives valuable insights on key focus points when dealing with criminal investigations (Lomas, 2023).

2. MTI Background

MTI was a network or multi-level marketing scheme that claimed to offer automated trading services via bots, on behalf of its members, in cryptocurrency derivatives. The scheme promised a consistent monthly 10% return to members. The website shut down in December 2020, and the CEO, Johann Steynberg, vanished and fled the country. Steynberg was arrested on 29 December 2021 in Brazil, and returned to South Africa, one year after his disappearance, for allegedly presenting fake identification to law enforcement officers. It was then discovered that he is a wanted person, the CEO of MTI, by South African Police Services (SAPS). At the time of writing, the legal process is still in progress. A trusted source with knowledge of the case has reported to MyBroadband that over 46, 000 Bitcoin passed through the scheme (Vermeulen, 2022).

TCG Forensics is one of the main investigators on several MTI cases. This paper has been written in collaboration with TCG Forensics and one of their main investigators on crypto crime cases, Thor Pederson. Section 3 explains the use case selection and gives a high-level overview of the MTI dashboard and platform functionality.

3. Use Case Selection

Anonymous ZA, a hacker group, released explosive details regarding the scheme, or rather the scam, on a Github link, MTI-Leaks (MTI-Leaks, 2022). Information such as their balance sheet, wallet addresses of founding members and members who benefitted the most from the scheme, the amount of Bitcoin allocated to the top addresses, withdrawals, cancelled and reversed withdrawals, remaining capital, the total money owed to members, etc. have been released. *Anonymous* also revealed that a handful of members received a "Founders Pool" bonus. Only 63 members were designated as founders, 0.038% of the total userbase (Vermeulen, 2020). This use case was selected from the MTI-Leaks website. The personal information of the target person will not be revealed but the initial address into which the target person invested will be revealed. It should be noted that the selected person of interest is not one of the founders of MTI, or the so-called masterminds of the scheme.

On the MTI Dashboard, the member was able see his/her portfolio with the total number of team members under the member's name, as well as the total direct referrals, the all-time bonusses, binary bonusses, the total wallet or account balance in MTI, and the total pool balance. The selected target person had 44419 team members, with 21 direct referrals, as illustrated in Figure 1. The member had 21783 members with 362.27 Bitcoin (BTC) in total on the left leg and 22636 members with 968.64 BTC on the right leg of the team (see Figure 2). Clearly the target person benefitted immensely from the scheme and qualifies as a person of interest. A high-level investigation has been conducted to trace the funds that were added/withdrawn to/and from the scheme.

Figure 1. Total Team Members and Direct Referrals

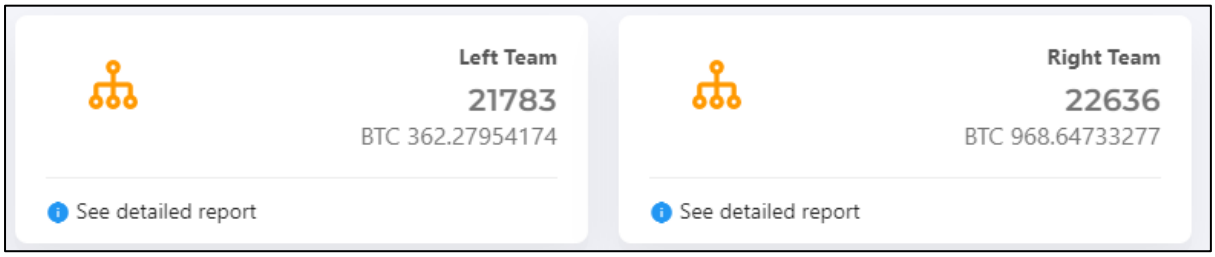

Figure 2. Left and Right Leg of Team

From the MTI dashboard, the user had a wallet section where an audit of funds added and withdrawn was kept. The investigation therefore has two angles:

1. Tracing the funds starting from the add funds address(s), the **Inputs**, and
2. starting from the withdrawal addresses(s), the **Outputs**.

The "**Add Fund History**" menu option on the dashboard (Figure 3) shows all five records recorded on the platform were selected as **inputs**. Note that the wallet address and transaction ids (TXIDs) are from the Bitcoin blockchain (

Table 1).

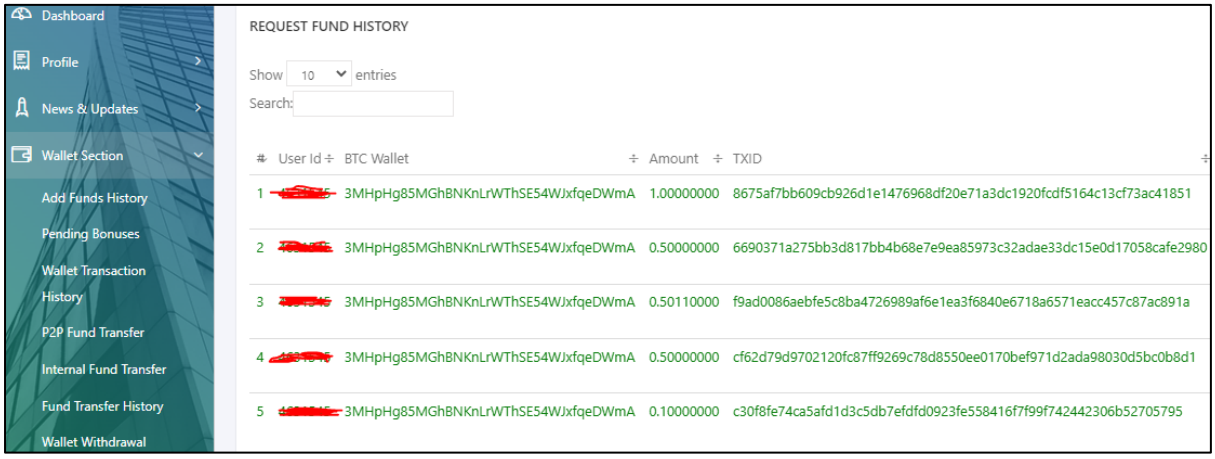

Figure 3. MTI Dashboard Menu (From MTI-Leaks)

Following the "Wallet Withdrawal" menu option from the dashboard, the very first withdrawal record was selected, Out-Address-1. However, this address had no TXID linked to it on the blockchain. A second address was selected, the first one from the list with a TXID linked to Out-Address-2. The third address selected was the most address used for pay-outs (Out-Address-3), with five transactions to start off with tracing the funds (see Table 2). These addresses are placed within the Outputs angle of the investigation.

According to Pederson, from TCG Forensics, the process for investigating a cryptocurrency scheme is dependent on the information available both publicly and during the course of the investigation. Before beginning the investigation, it is of utmost importance to collect all information that will enable the investigator to develop, compile and expose a timeline. An example of this could be a specific user or investor in a scheme that may have information very pertinent to the investigation process. An investor knows that over the course of the operation of the scam, the scam required deposits into a specific cryptocurrency address and that address changed over the course of a few months. This information alone information is extremely valuable and has a massive impact on where and when to investigate, and to find or join links over time (TCG Forensics, 2022).

Table 1. Inputs

Wallet Address	TXID	BTC	Date
3MHpHg85MGhBNKnLrWThSE54WJxfqeDWmA **(In-Address-1)**	8675af7bb609cb926d1e1476968df20e71a3dc1920fcdf5164c13cf73ac41851 **(Input-TXID-1)**	1	2020.05.17
3MHpHg85MGhBNKnLrWThSE54WJxfqeDWmA **(In-Address-1)**	6690371a275bb3d817bb4b68e7e9ea85973c32adae33dc15e0d17058cafe2980 **(Input-TXID-2)**	0.5	2020.03.29
3MHpHg85MGhBNKnLrWThSE54WJxfqeDWmA **(In-Address-1)**	f9ad0086aebfe5c8ba4726989af6e1ea3f6840e6718a6571eacc457c87ac891a **(Input-TXID -3)**	0.5011	2020.03.29
3MHpHg85MGhBNKnLrWThSE54WJxfqeDWmA **(In-Address-1)**	cf62d79d9702120fc87ff9269c78d8550ee0170bef971d2ada98030d5bc0b8d1 **(Input-TXID -4)**	0.5	2020.03.21
3MHpHg85MGhBNKnLrWThSE54WJxfqeDWmA **(In-Address-1)**	c30f8fe74ca5afd1d3c5db7efdfd0923fe558416f7f99f742442306b52705795 **(Input-TXID -5)**	0.1	2020.03.21

Table 2. Outputs

Wallet Address	TXID	Amount (BTC)	Date
1KX5f1mz8MBuCCdUyDcyRiZLH53v8cJjav (First address – **Out-Address-1**)	Not available	1.005	2019.12.12 23:06:20
3CvyH1syeBrJWLXkXpXtQtJ82wVq5naocV (**Out-Address-2)** (First Address with TXID)	7572ccc5c31b65e2eb72f62d78d42ec3ca20cf93884ec0e7664722ed54c4aa3c **(Output-TXID -1)**	2.5	2020.05.11 21:43:39
17AVMgsdxb7tELKwjn4fK3MymGkUTmY6DB (**Out-Address-3)** Most common used address	58c0b545a0eac027d143eb0838fe3b59fb093d1d383124b2f80893aaf00e697d **(Output-TXID -2)**	0.3	2020.07.19 22:58:01
	734e6394a4bda9de8707cdcca2e8760ef028f4a33b6845b32923ed918170a91c **(Output-TXID -3)**	0.27867493	0.27867493
	b92242994510d45a2dd12c1f9f2f89034f1870252839d066f6050db951153d12 **(Output-TXID -4)**	2020-07-20 03:00:25	2020.07.20 03:00:25
	d3d743092c6968cc255c631f0179b000e0a664328642e8921ace3c6ca30e95e2 **(Output-TXID -5)**	0.61480277	2020.07.26 22:47:06
	885700b5c8978d1c0267244a9a69ab41009e2ef1569a611c4a8d535321d35eec **(Output-TXID -6)**	0.1	2020.07.28 21:17:17

The second most important element is the flow of funds. The flow of funds is defined as the start and end points. In simple terms this means where the funds started, where they travelled, what happened to them and where they exited and all common points for such funds along the journey. Bad actors will deliberately attempt to obscure the flow of funds from investors and interested parties. The flow of funds is dependent on the type of scheme that was in operation. In the case of an investment scheme, one would expect to follow the path of the deposited funds to an investment vehicle on the blockchain, and this in itself may take on many forms such as crypto mining, token exchanges, trades, etc. Furthermore, it is not always possible to extrapolate the truth without confirmation that what one may find on the blockchain will concur with what was advertised to the investors (TCG Forensics, 2022).

4. High-level Proposed Process

Several engagements took place with TCG Forensics to determine a high-level process an investigator could follow to investigate a crypto scam. The focus was specifically on the MTI scam with the given data obtained from MTI-Leaks, but it could be applied to various forms of crypto scams, crimes, money laundering and fraud.

Seven steps have been identified as an initial high-level process, applicable for both the input and output addresses. The steps are outlined listed below and outlined in**Error! Reference source not found.**:

1. Identify the input addresses and the output or pay-out addresses.
2. Follow the funds on the blockchain starting from the identified addresses.
3. Identify key or common addresses used, their function and determine if they are linked to exchanges.
4. Further follow the funds from the key or common addresses identified.
5. Determine if there are any correlations between the addresses identified, such as a certain address being used as a destination address, linkages to exchanges, etc.
6. Identify the destination addresses.
7. At this point, legal support is required. Below are five key points to address when drafting legal charges:
    a. Draft a forensic report detailing the scam.
    b. Report to the Financial Sector Conduct Authority (FSCA).
    c. Draft the legal charges.
    d. Formulate and issue a subpoena on the identified linked exchanges and obtain the KYC identification documents.
    e. Freeze the funds linked to the destination addresses if possible.

Figure 4 illustrates the process.

5. Analysis and Investigation of the Selected MTI Case

The high-level process detailed in section 1, and drafted in **Error! Reference source not found.**, was used as a base and a guide to perform the analysis and investigation on the selected target person, who was a member of the MTI Ponzi scheme and benefitted tremendously out of the scheme. The target person is expected to repay the funds after the investigation and the required legal steps have been taken to finalise this case.

The crypto investigation tool, QLUE, was used to perform the investigation and to follow or trace the funds on the blockchain. (QLUE, 2022) Inputs and outputs almost never come from the same source (TCG Forensics, 2022). It is very difficult without sufficient context to know to whom a Bitcoin address belongs when using a crypto wallet (Lomas, 2023). However, the aim of this investigation is to follow the transaction flow on the blockchain, to determine patterns, to find key addresses where money was transferred to and from, and identify when a transaction was made to an exchange.

5.1 Inputs

The first part of the investigation is to investigate the funds being added onto the platform and by following the input transactions up to a point where they are linked to an exchange and a person can be identified.

Step 1

The input addresses have been identified from the MTI "**Add Fund History**" option and are listed in Table 1. Also refer to Figure 3.

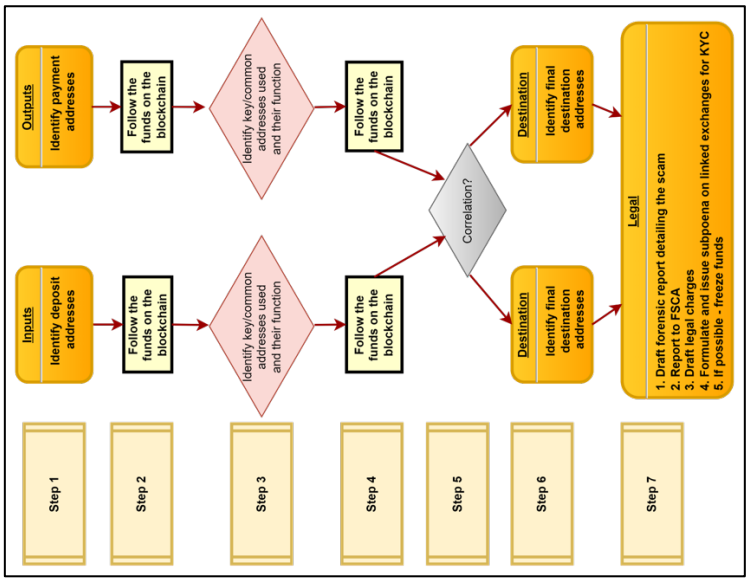

Figure 4: Investigation Process

Step 2 & Step 3

This investigation starts off with entering the input address, **In-Address-1**, into QLUE. Upon entering the input address, **In-Address-1**, QLUE returned no results and this immediately raised a red flag. The absence of results can mean no such address exists on the Bitcoin blockchain or no transaction has been made into the address. The next step was to confirm this on the online blockchain explorer, Blockchain.com (Blockchain.com, 2022). When entering the address into the explorer, the address does exist, but no transaction was ever made to this address. This may indicate the MTI administrators possibly intended to use this address as a dummy, and never reveal to the public where the funds actually went.

When entering the first input TXID, **Input-TXID-1** from
Table 1, it was discovered that the funds went to a different address than what was indicated on the MTI platform, and that it was a Bitcoin address that had been flagged by QLUE as a MTI address (refer to Figure 5 below - note that the green arrow indicates funds being received and the red arrow indicates funds being sent). This address will be referred to as **MTI-1**, as indicated in Figure 5. When following the funds further, another interesting discovery was that the funds went out of **MTI-1** to another address, on the very same day, approximately 3.5 hours later. Hereafter, the funds were sent to thousands of addresses. This indicates that mixer or tumbler services were possibly used.

When analysing **Input-TXID-2** and tracing the funds, it was revealed that the funds were transferred to a different MTI Bitcoin address, **MTI-2**, from **Input-TXID-1**. **Input-TXID-3** also went to **MTI-2** (refer to Figure 5).

Input-TXID-4 went to another MTI address, **MTI-3**, and **Input-TXID-5** went to **MTI-4** (refer to Figure 6).

Step 4 & Step 5

Upon further investigation and tracing of the funds, the tool revealed that thousands of transactions occurred after funds had been moved to these identified addresses. Considering **MTI-1** as an example, it indicates that from this address alone, 6K more transactions occurred. From **MTI-2**, 2K additional transactions occurred. Upon expanding **MTI-2**, only 53 transactions were made visible in QLUE, due to filtering applied, out of the 2K transactions shown in Figure 7. This indicates that MTI was possibly making use of crypto mixing to anonymise the crypto transactions. Crypto mixing or crypto tumblers is the process of obscuring the origins of a crypto transaction through mixing one's tokens with others of the same type. This results in thousands of transactions, with the goal to confuse the investigator, leaving multiple trails and paths of transactions on the blockchain (CryptoHopper, 2022). By using the tool QLUE, these traces have been followed and further key or common addresses have been identified. Key findings from the inputs were that funds were sent to a few common addresses linked to the MTI scam.

Step 6

Another noticeable finding was that after thousands of transactions had been made to several MTI linked addresses and other random addresses, funds were transferred to South-African exchanges such as Luno, VALR and AltCoinTrader. Funds were also transferred to exchanges outside of SA, such as Binance, Coins, Nexo, etc. The addresses on the South African exchanges have been marked in this investigation as the destination addresses, **Destination1** and **Destination2** (refer to Figure 7).

Step 7

Depending on the jurisdiction there are legal steps one is obliged to follow which are common to most countries. As such inter-agency or inter country co-operation can and often is requested by the investigator normally based on the submission of a thorough blockchain forensics report and backed by law enforcement authorities. Depending on the country from which cooperation is requested, a specific process may be required to be followed. Typically, the process may involve issuing subpoenas on the relevant exchanges via their compliance officer which often results in the investigator obtaining the required personal information from the identified exchanges. Once the target person has been identified, a notice should be sent to the person of interest, with a warning and court order that the funds linked to the person's name in certain specific identified addresses are not allowed to be moved. An instruction could be given to the exchanges to freeze the account for a time period, this normally requires the submission of the correct court processed documentation and proof of legal authority to act on behalf of the aggrieved. Should the account holder reside in the country where the investigation is being conducted, a court application can be made in order to instruct the account holder to cease and desist

from all activity on the blockchain account pending a court action against them, and violation of the court order is often backed up by contempt of court charges. In this event, the account holder will get a legal notice not to move any of the funds within these addresses (TCG Forensics, 2022). It should be noted that these people could highly likely be low-level mules and located in a different jurisdiction. To make an arrest, more context and other thresholds will be needed to get to the actual arrest point (Lomas, 2023). From this point, it becomes a legal case. If a decision is made by the court, funds could be moved and recovered as instructed by officials.

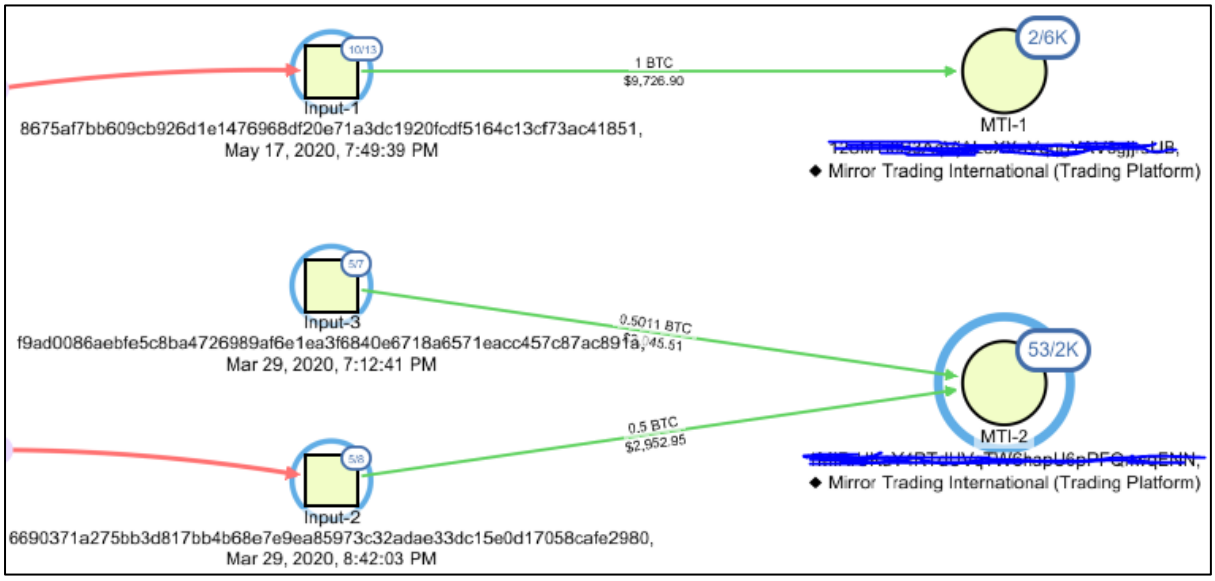

Figure 5. Input-1, 2 & 3

5.2 Outputs

The second part of the investigation is to investigate the pay-outs or outputs by following the output transactions up to a point where a person can be identified.

Step 1

The output addresses have been identified from the MTI Dashboard "Wallet Withdrawal" menu option and listed in Table 2. Also refer to Figure 3.

Step 2 & Step 3

By entering the first output address, Out-Address-1, into QLUE and following or tracing the funds, the tool revealed that four transactions are linked to this address even though MTI indicated no transaction is linked to this address; two input transactions with 0.005BTC and two output transactions with the same amount were found. MTI indicated that the amount that was transferred into this address is 1.005BTC. The sum of the four transactions found on the blockchain does not add up to this amount from the MTI platform, which already raises some questions. The two input transactions to Out-Address-1 that were identified are:

- b169639976a598029999191e0fc255114169286da756ce421f31e92620fe24b5 (Out-Address-1-Input-TXID-1) and
- 372f1b3f6b8d5c4f504a0cdb6371c427464e119d4382eb70adefbdecdaf6c120 (Out-Address-1-Input-TXID-2).

These two transactions would need to be backwards traced to determine from where the funds came. Upon tracing Out-Address-1-Input-TXID-1 for several transactions backwards, it was discovered there are several links to local South African exchanges as well as international exchanges. Upon tracing Out-Address-1-Input-TXID-2 backwards, no destination addresses could be identified, however, a single path could be followed that was ultimately linked to several exchanges.

The two output transactions to **Out-Address-1** that were identified are:

- dc4de50957a2a64a84a2a7d410155a6456083d365696fed9db0af6f015f62b40 (Out-Address-1-Output-TXID-1) and

- c8c4c08467e86fbe572d130c268b94711d51f475c196a76b32d949c3cb8ce5d8 (Out-Address-1-Output-TXID-2).

These two transactions need to be traced forwards in order to determine where the funds moved to, with the aim of finding a destination address.

When moving on and tracing **Output-TXID-1**, QLUE revealed that the funds were moved to blockchain addresses on both the Luno and AltcoinTrader platforms (see Figure 8). However, none of the addresses clustered in Luno and AltcoinTrader matched the address shown on the MTI dashboard that is supposed to be linked to **Output-TXID-1**. **Out-Address-2** is in fact linked to the Bitmex exchange and not linked to **Output-TXID-1** at all.

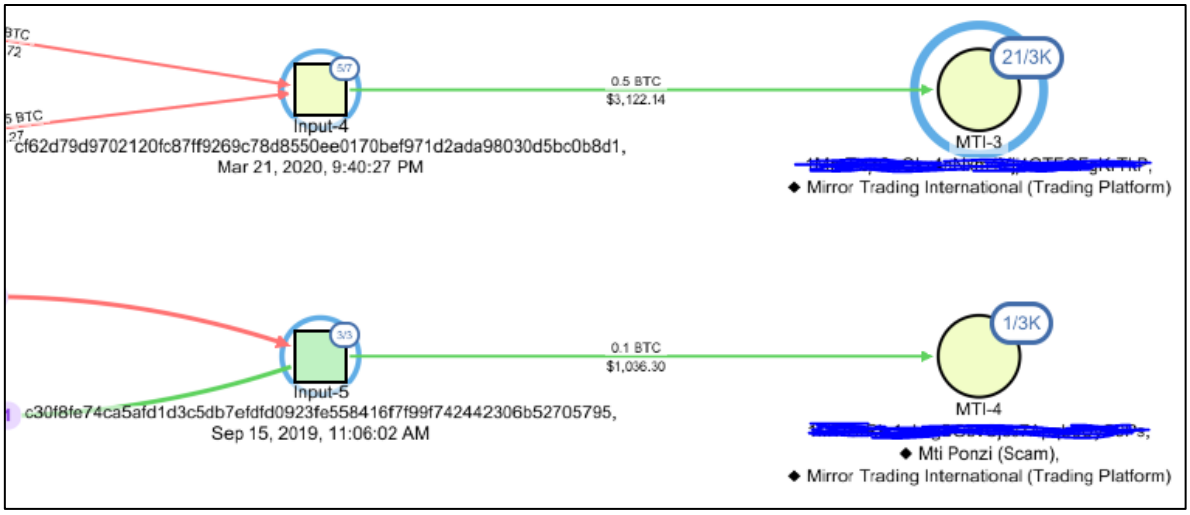

Figure 6. Input-4 & 5

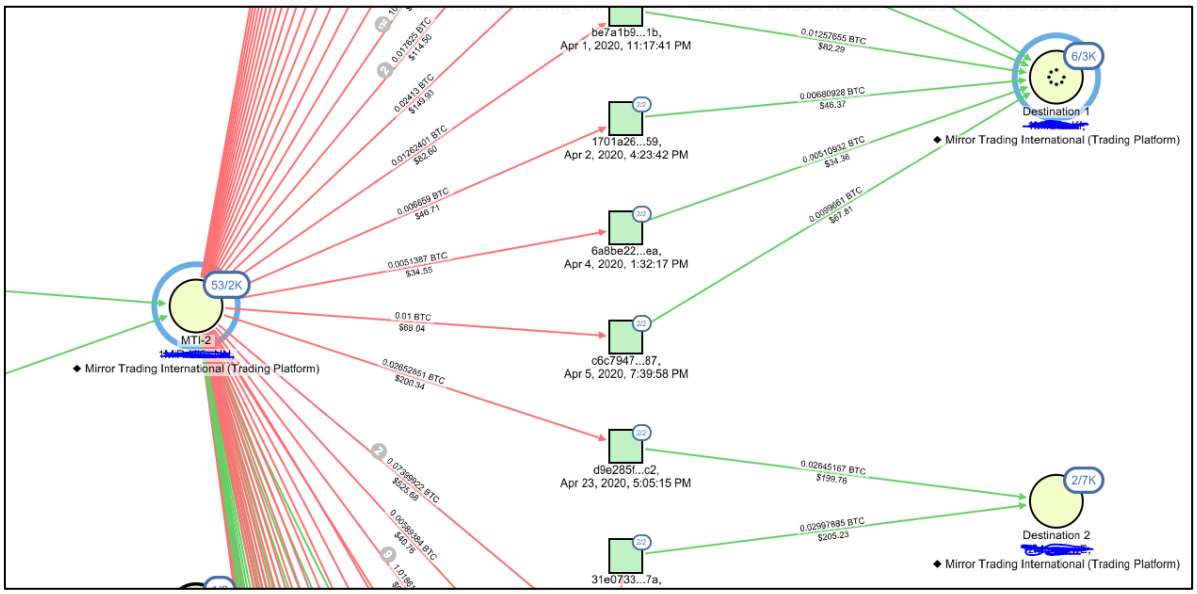

Figure 7. MTI-2 -> Destination 1 & 2

When tracing the most common used address from the MTI platform on the target person's profile, **Out-Address-3**, it revealed that the address was indeed linked to transaction **Output-TXID-5**, but not linked to any of the other transactions that MTI indicated are linked to the address. This indicates that the information shown to the members on the MTI dashboard is incorrect in this instance. The address has also been flagged by QLUE as a known MTI user address.

When tracing Output-TXID-2 via QLUE, no results came up. Another test was done using the tool Maltego (Maltego, 2023) with the Tatum transform for integrating with the blockchain. By tracing the input and output addresses via Maltego, several addresses were linked to the transaction (Figure 9), however none were the address shown on the MTI dashboard (see

Table 2). These addresses have been flagged for further investigation.

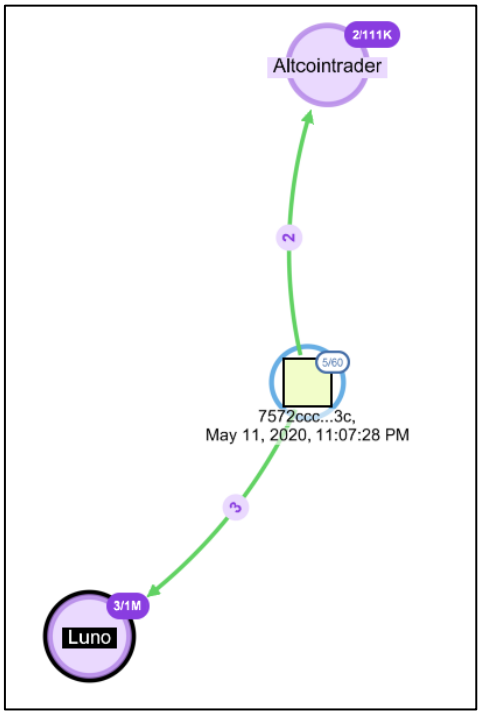

Figure 8. Output TXID-1

Step 4, Step 5 & Step 6

After further tracing on the **Out-Address-1-Input-TXID-1** path, a few addresses have been identified and linked to a number of exchanges such as Binance, Coinhako, Altcoin Trader, Unocoin wallet exchange and Coins exchange. When tracing the path backwards from **Out-Address-1-Input-TXID-1**, a correlation could be made to the exchanges Coinpayments, Bitmex, Bitpoint and Binance, as well as links to Dark Market activities based on the flagged addresses by QLUE. These addresses have been flagged as destination addresses for further investigation.

By following **Out-Address-1-Output-TXID-1** forward, several links to exchanges such as Bitstamp, BitPay, Paymium, Bitrex, Bitmex, Binance, Changelly, Hitbtc, Bitcoincom and Bithoven have been discovered. When tracing **Out-Address-1-Output-TXID-2** forward it was discovered that the two output transactions have a correlation on a particular transaction id that serves as an output for **Out-Address-1-Output-TXID-2** and is also an input for **Out-Address-1-Output-TXID-1**. QLUE has also clustered the two addresses together from the two outputs, which could indicate that these addresses belong to the same exchange or are controlled by the same person. These addresses have been flagged as destination addresses for further investigation.

The Bitmex address, **Out-Address-2** has been flagged as a destination address. The addresses linked to Luno and AltcoinTrader from **Output-TXID-1** have also been marked as destination addresses for further investigation.

The addresses linked to **Output-TXID-3**, **Output-TXID-5**, **Output-TXID-5** and **Output-TXID-6** have all been marked as destination addresses for further investigation. The addresses linked to **Output-TXID-6** have been flagged with a high priority as they indicate links to a known MTI user address as well as links to victims of fraud.

Step 7

Depending on the legal jurisdiction there are legal steps one is obliged to follow or request inter-agency co-operation - refer to section **Error! Reference source not found.**, Step 7 (TCG Forensics, 2022). By issuing subpoenas to the relevant exchanges via the compliance officer, the investigator could obtain personal information from the identified exchanges. If two or more of the addresses have the same personal information, there is a high possibility that the personal information is that of the target person. Similar to Step 7 in section **Error! Reference source not found.**, an instruction could be given to the exchanges to freeze the account. Legal notices and/or charges will follow, and the court will come to a final decision on what should happen to the funds. Again, it should be noted that these identified target persons could possibly be low-level mules and not the main target person of the scam (Lomas, 2023).

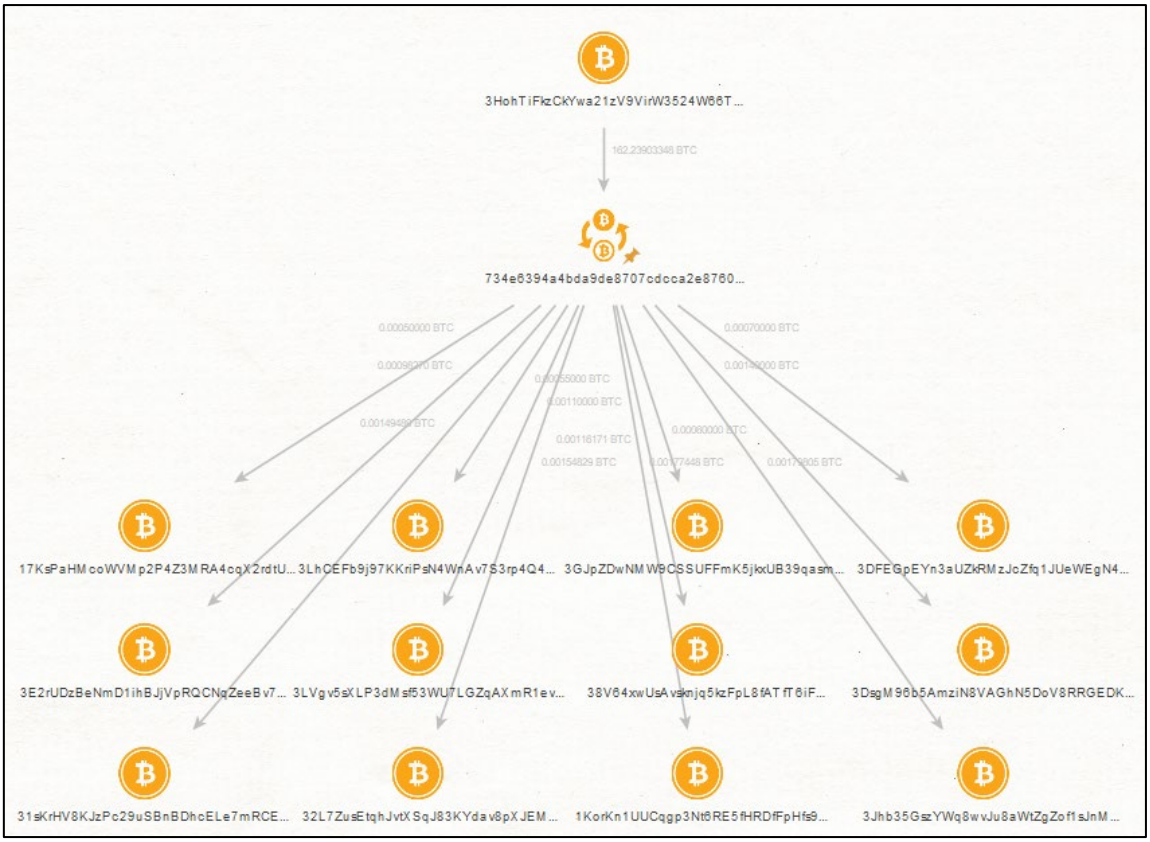

Figure 9. Output-TXID -2 - Linked Addresses

6. Conclusion

This paper focusses on a selected target person that was a member of the MTI scam who has benefitted immensely from the scam. MTI-Leaks has been used for the case selection and the data on input and output transactions and the addresses linked to them. Several discussions took place between the first author and a of crypto crime investigator from the South African company, TCG Forensics. The aim of the discussions is to propose a high-level process on how to investigate crypto scams and crimes. This process is presented in this paper and used as a base line to perform a high-level investigation. Limited free access to the tool QLUE has been obtained to perform the investigation. In addition, Jeff Lomaz, an OSINT and crypto crimes investigator from the USA, gave valuable insights on online criminal investigations.

The investigation followed two approaches, one for the funds being added onto the MTI platform, referred to as the inputs, and the second approach considers the fund withdrawals from the platform, referred to as the outputs, which are the pay-outs. After numerous efforts to trace the funds on all Bitcoin addresses and transactions that were selected from the MTI dashboard on the target person's profile, several addresses have been marked as the destination addresses and for further investigation. After the identification of the destination addresses, depending on the jurisdiction, subpoenas could be issued to the linked exchanges in order to obtain personal information on the individuals who performed the transactions on the particular exchanges. Further legal steps would then take place until a decision has been made by the court.

The crypto industry continues to grow, and criminals will continue to scam individuals and launder proceeds of their crimes using cryptocurrencies. The continued advancements in the blockchain and crypto industry make it more challenging for law enforcement agencies to detect and fight criminal activity. At the same time, it will be even more challenging for criminals to launder illegally obtained funds. It is important for governments, competent authorities, and law enforcement agencies to stay up to date with the methods adopted by criminals and to take advantage of blockchain analytic tools to effectively combat money laundering with the use of cryptocurrencies and crypto assets.

References

Blockchain.com. (2022, 12 14). *Blockchain.com - Explorer*. Retrieved from Blockchain.com: https://www.blockchain.com/explorer

Chainalysis. (2021). *The 2021 Crypto Crime Report.* Chainalysis. Retrieved from https://go.chainalysis.com/rs/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf

Connors, C. (2022, 12 09). *What is a Cryptocurrency Investigation?* Retrieved from ERMProtect.com: https://ermprotect.com/blog/what-is-a-cryptocurrency-investigation

CryptoHopper. (2022, 8 23). *What is crypto mixing?* Retrieved from www.cryptohopper.com: https://www.cryptohopper.com/news/7547-what-is-crypto-mixing

Lomas, J. (2023, 01 12). *Certified Instructor - Jeff Lomas*. Retrieved from sans.org: https://www.sans.org/profiles/jeffrey-lomas/

Maltego. (2023, 01 14). *Home page*. Retrieved from maltego.com: https://www.maltego.com/

MTI-Leaks. (2022, 11 24). *Mirror Trading International Data Leak*. Retrieved from MTI-Leaks: https://mtileaks.github.io/

QLUE. (2022, 11 25). *QLUE*. Retrieved from qlue.io: https://qlue.io

Sigalos, M. (2022, 01 7). *Crypto scammers took a record $14 billion in 2021*. Retrieved from cnbc.com: https://www.cnbc.com/2022/01/06/crypto-scammers-took-a-record-14-billion-in-2021-chainalysis.html

Social Links. (2022, April 22). *Enhancing Cryptocurrency Investigations with OSINT*. Retrieved from https://blog.sociallinks.io/: https://blog.sociallinks.io/cryptocurrency-investigations/

Stylianou, A. (2022, 4 4). *CRYPTOCURRENCIES - THE CHALLENGES FOR CRIMINALS AND INVESTIGATORS*. Retrieved from www.gci-ccm.org/: https://www.gci-ccm.org/insight/2022/04/cryptocurrencies-challenges-criminals-and-investigators

TCG Forensics. (2022, 11 28). *Home page*. Retrieved from www.tcgforensics.co.za: https://www.tcgforensics.co.za/

Vermeulen. (2022, 4 12). *Good news for Mirror Trading International scam victims*. Retrieved from mybroadband.co.za: https://mybroadband.co.za/news/cryptocurrency/440928-good-news-for-mirror-trading-international-scam-victims.html

Vermeulen, J. (2020, 9 20). *Explosive information about Mirror Trading International released by Anonymous ZA*. Retrieved from https://mybroadband.co.za/: https://mybroadband.co.za/news/business/368165-explosive-information-about-mirror-trading-international-released-by-anonymous-za.html

Xia, P., Wang, H., Luo, X., Wu, L., Zhou, Y., Bai, G., . . . Liu, X. (2020). Don't Fish in Troubled Waters! Characterizing Coronavirus-themed Cryptocurrency Scams. *2020 APWG Symposium on Electronic Crime Research (eCrime)*, (pp. 1-14). doi:10.1109/eCrime51433.2020.9493255