An Analysis of a Cryptocurrency Giveaway Scam: Use Case

Johnny Botha[1] and Louise Leenen[2]
[1]Council for Scientific and Industrial Research, Pretoria, South Africa
[2]University of Western Cape and CAIR, Cape town, South Africa

jbotha1@csir.co.za
lleenen@uwc.ac.za

Abstract: A giveaway scam is a type of fraud leveraging social media platforms and phishing campaigns. These scams have become increasingly common and are now also prevalent in the crypto community where attackers attempt to gain crypto-enthusiasts' trust with the promise of high-yield giveaways. Giveaway scams target individuals who lack technical familiarity with the blockchain. They take on various forms, often presenting as genuine cryptocurrency giveaways endorsed by prominent figures or organizations within the blockchain community. Scammers entice victims by promising substantial returns on a nominal investment. Victims are manipulated into sending cryptocurrency under the pretext of paying for "verification" or "processing fees." However, once the funds have been sent, the scammers disappear and leave victims empty-handed. This study employs essential blockchain tools and techniques to explore the mechanics of giveaway scams. A crucial aspect of an investigation is to meticulously trace the movement of funds within the blockchain so that illicit gains resulting from these scams can be tracked. At some point a scammer wants to "cash-out" by transferring the funds to an off-ramp, for example, an exchange. If the investigator can establish a link to such an exchange, the identity of the owner of cryptocurrency address could be revealed. However, in organised scams, criminals make use of mules and do not use their own identities. The authors of this paper select a use case and then illustrate a comprehensive approach to investigate the selected scam. This paper contributes to the understanding and mitigation of giveaway scams in the cryptocurrency realm. By leveraging the mechanics of blockchain technology, dissecting scammer tactics, and utilizing investigative techniques and tools, the paper aims to contribute to the protection of investors, the industry, and the overall integrity of the blockchain ecosystem. This research sheds light on the intricate workings of giveaway scams and proposes effective strategies to counteract them.

Keywords: Blockchain, Crypto-crime, Cryptocurrency, Crypto-scam, Giveaway-Scam.

1. Introduction and Background

Cryptocurrencies continue to grow by means of legitimate users, but they also attract a wide range of criminal activities (Pelker, 2021). Cryptocurrency (crypto) giveaway scams are one of the most common scams in which an attacker lures a victim by announcing a giveaway of a certain cryptocurrency or digital asset (Botha, Badenhorst, & Leenen, 2023). These types of scams have been a major problem for the crypto community since late 2017. It is recommended that all crypto investors be educated on current crypto related scams in order to identify such instances. A giveaway scam is a form of social engineering where a scammer attempts to deceive an investor in believing some major crypto currency exchange, such as Coinbase[1] or Binance[2] for example, is hosting a giveaway. To participate in the giveaway, the investor is requested to send a specified amount of cryptocurrency to a given address so that the platform can verify the investor's wallet address and the legitimacy of the investor's account. It should be noted that crypto transactions are irreversible; once the victim has sent funds to the scammer's address the transaction cannot be reversed. It should also be noted that exchanges host actual giveaways from time to time, but these exchanges never issue requests for cryptocurrency contributions to participate in giveaways (Hauer, 2020).

Scammers make use of social media sites to advertise or announce their fake giveaways. A giveaway scam is often linked to an impersonation scam. Scammers will either impersonate a company, a celebrity or a famous influencer. An example of a scam where a company is impersonated, may involve a Twitter account supposedly belonging to the Coinbase company. In this scam a 5000 Bitcoin (BTC) giveaway scam is promoted by a tweet containing a link which redirects users to a fraudulent web page. The target is asked to send any amount from 0.1 to 10 BTC to the scammer's giveaway address in order to verify the target's address. On the web page, targets are assured that they will earn ten times their "verification"payment. In reality, a victim will not receive any payback – they have fallen for a scam. The impersonation of an individual is any instance in which a scammer tries to take advantage of a famous person's trustworthy reputation on social platforms such as Facebook, Twitter, YouTube, Telegram, Discord, Instagram, TikTok, etc. Celebrities who have often been impersonated in

[1] https://www.coinbase.com
[2] https://www.binance.com

giveaway scams in recent years are, for example, Elon Musk, Michael Saylor, and others. The scammer will pretend to have benefited from a giveaway by supposedly thanking the impersonated celebrity in a tweet. An example is shown in Figure 1; an image of a tweet, supposedly posted by Musk, promotes a cryptocurrency giveaway being hosted by Tesla. However, the image was manipulated and did not originate from Musk. The link in the scammer's image redirects a user to a landing page that appears to be from Tesla or Mr Musk offering "free" Bitcoin and Ethereum (Hauer, 2020).

Figure 1: Celebrity Twitter Impersonation (Hauer, 2020)

Another method scammers use is to send a direct message (DM) on a social media platform, pretending to be a celebrity or an ambassador of that celebrity, advising a potential victim to participate in some crypto investment or giveaway. When a victim engages, he is requested to send a WhatsApp message to a given cell phone number so assistance can be provided. This approach may appear to be more personal to the victim and will contain a link where more details on participation will be provided. Figure 2 shows a website to which the potential target is directed - a photo of the individual being impersonated is shown. When a target opts in, a crypto address will be provided where the crypto coins can be sent in order to participate and to receive, for example, double the rewards in return. This scam continues after the victim has sent the money; the attacker will send fake proof of supposed profits generated and then request a withdrawal fee for payment of the reward. By the time the victim realises he has not received any payment even after he has paid the withdrawal fee, it is too late. The person has fallen victim to a crypto giveaway scam (Bureau, 2022) (Guez, 2023).

YouTube live streams is a new technique being used by scammers to lure victims. A scammer creates a YouTube video, using an older video stream of an interview with a famous person or CEO or a company. The scammer will then overlay the video with the details of the giveaway promotion. The scammer will set up the video as a current live stream so that it appears the giveaway is happening currently, enticing viewers to participate immediately. A link or QR code is normally provided in the description of the video, directing the viewer to a web page with more details on the fake crypto giveaway. Furthermore, it will also appear as if thousands of people are participating in the livestreams. However, these are generally bots and not real people. The YouTube account will often also appear to have been verified. In these cases, the accounts were hacked, all contents were deleted, and the attackers are running their own livestreams. Another way of launching this type of attack is when an attacker runs advertisements that appear around legitimate videos. If a targets clicks on one of these advertisements he is transferred to a fake site. Figure 3 contains a screenshot of a YouTube live stream using a video of an actual interview with the CEO of Coinbase, Mr Brian Armstrong.

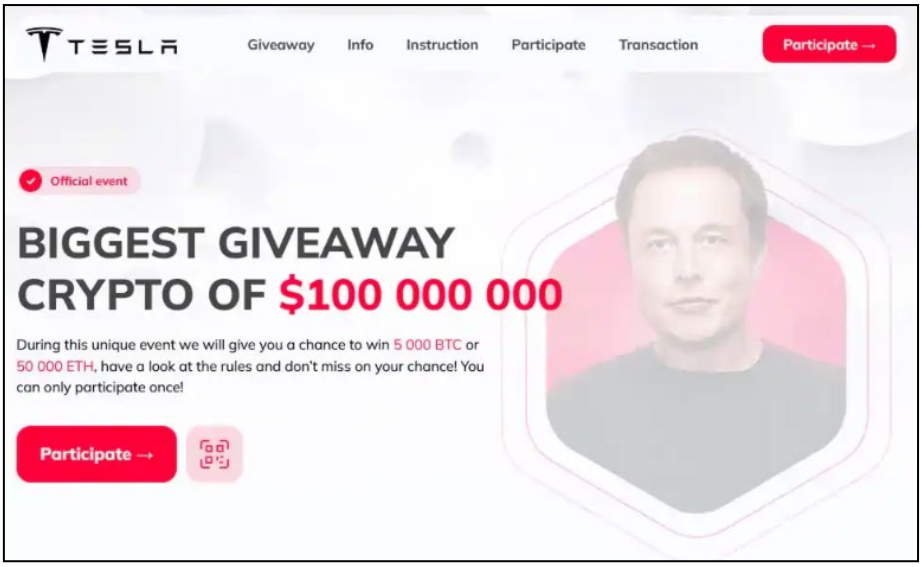

Figure 2: Tesla Crypto Giveaway (Guez, 2023)

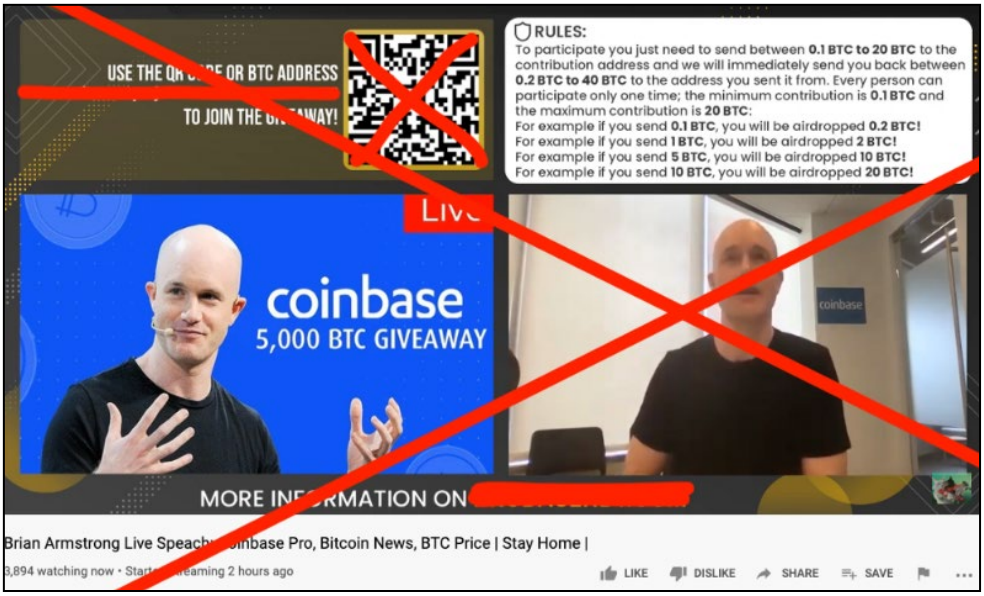

Figure 3: YouTube Live Stream

Another, more traditional way in which scammers lure their victims is via email. The scammer sends a phishing mail attempting to convince a user that a crypto giveaway is being hosted. The user clicks on a provided link and participates.

Scammers have been around long before crypto, but they find some of the characteristics of crypto very appealing. Crypto has no middleman as in the case with bank transactions. Instead, direct transactions occur between two individuals. Crimes in the cryptocurrency space victimise innocent people - it places a big barrier on further adoption rates and increases government restrictions. 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).

This paper contributes towards the body of knowledge by raising awareness of crypto giveaway scams. In addition, the study illustrates how an investigator can analyse and investigate this type of scam, on the blockchain, using various tools and techniques. The paper further highlights how a user can be protected against these attacks. Blockchain is a revolutionary technology with immense benefits. However, the technology attracts criminals and poses an international crisis. In Section 2, a use case is selected and described. In Section 3, this

use case is investigated and analysed. Section 4 contains some recommendations and the paper is concluded in the last section.

2. Use Case Selection

During our search for a relevant use case, various websites and data sources have been considered. Bitcoinabuse.com is known for providing good data on scams involving cryptocurrency. Bitcoinabuse.com has recently merged with Chainabuse.com and now offers more functionalities (BitcoinAbuse.com, 2024). Chainabuse is currently the leading platform for reporting malicious cryptocurrency activities (Chainabuse.com, 2024a). Upon filtering the results to only display impersonation scams, which are similar to giveaway scams, one particular scam impersonated Michael Saylor, the former CEO of Microstrategy (Forbes, 2024). The authors of this paper decided to select this scam as a use case because he is a popular figure in the crypto space, a billionaire with a net worth of $2.9 billion (as of 8 January '24), one of the biggest Bitcoin Maxis (a person who believes only Bitcoin is a true cryptocurrency) and one of the biggest Bitcoin holders via the company MicroStrategy (Chainabuse.com, 2024b). The scam is a recent case; it was reported on 6 January 2023. Two links are available to view more details on the scams in pdf format:

- https://bafybeic2yumotbzu6u36tkteckdceqrftfyqyye4xegczin5iufuh7nmaq.ipfs.w3s.link/mstrx2.com.pdf *(YouTube Live Stream).*
- https://bafybeihmck427mca37tkz22zpceglcrzpmvxr67bbt75o6telnvyzkqmay.ipfs.w3s.link/v%3DPaSQ5dZ25dg.pdf *(Web page).*

The two contributing crypto addresses are:

- 15YU4Pr3gDN78JjhgctKjRQ9NJhRdZn4Hf *(BTC)*
- 0x766352635223f86abe5C970bb1C199DF14099B8f *(ETH)*

The scam was announced on a YouTube Channel called Super DJ Sound where a live video of an interview with Mr Saylor, regarding the Bitcoin ETF approval, has been manipulated with added on information that took participants to the giveaway landing page. In the "chat" section on the channel, Mr Saylor was impersonated where he interacted directly with participants (Figure 4). The link to the actual video does not work anymore and has been removed.

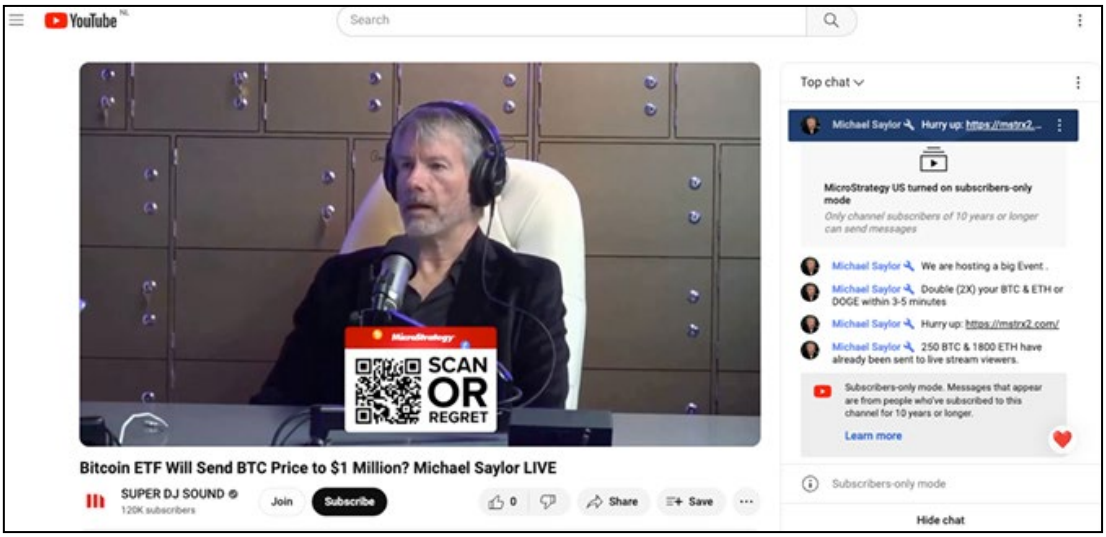

Figure 4: Live YouTube Video - Bitcoin ETF - Michael Saylor (Random Generated Link 1, 2024)

The channel displayed a QR code that takes the participant to a fake MicroStrategy website, http://www.mxstrx2.com. Instructions and rules are explained on the landing page, announcing that MicroStrategy would give away crypto assets to the value of $1 billion to participants (Figure 5). Note that the website looks exactly like the one from the Tesla giveaway example in Section 1, Figure 2 (apart from the photos of two impersonated individuals). This indicates that the same scammer is running multiple scams using the same website template and updating the content on multiple impersonations.

At the time of writing, Windows Defender reported the website to be unsafe and containing misleading content. However, the website can still be accessed if the warning from Microsoft Defender is ignored and one accepts the risks to visit the website. On the website, a giveaway of 1000 BTC and 10,000 ETH is promised. To participate, the user must send any amount between (0.1 BTC – 15 BTC) or (1 ETH – 200 ETH) to the contributing address, and MicroStrategy will then send back double the amount (0.2 BTC – 30 BTC) or (2 ETH – 400 ETH) to the address from which the payment was received. A list of supposedly successful transactions where users received double the paid amount, is shown on the landing page (Figure 6). It should be noted that these addresses in the transaction list are deliberately not displayed in full and those transactions cannot be verified (Random Generated Link 2, 2024). Section 3 covers an analysis and a technical investigation of the selected scam where the full addresses will be revealed as a result, and can be verified if the visible parts of the address match any of the addresses that are uncovered.

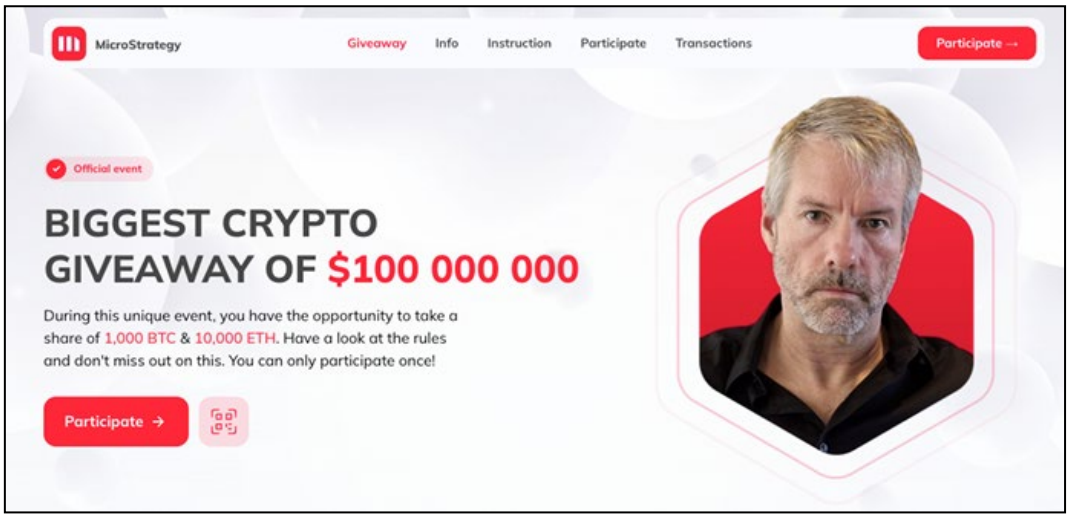

Figure 5: MicroStrategy Crypto Giveaway (Random Generated Link 2, 2024)

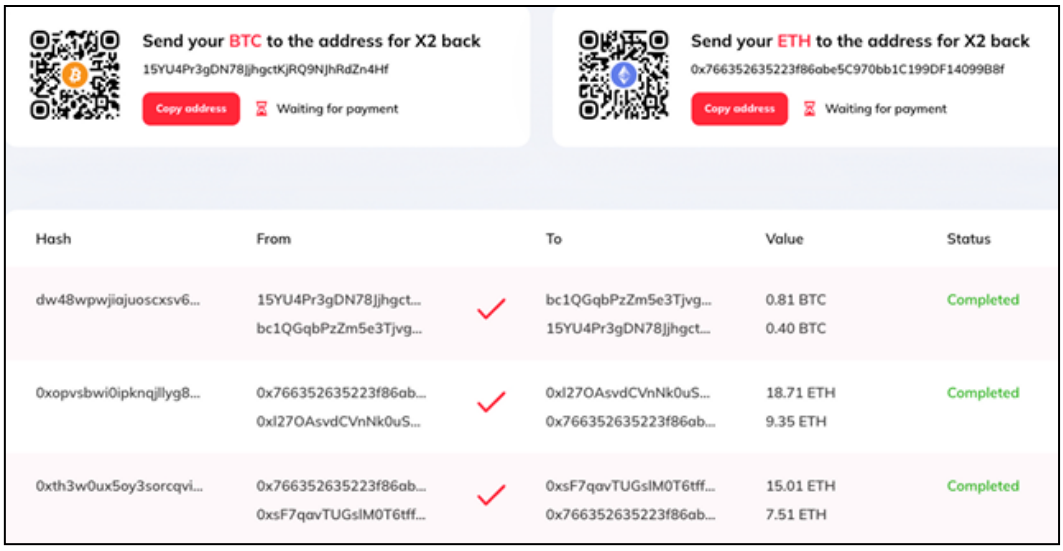

Figure 6: Completed Payback Transaction List (Random Generated Link 2, 2024)

3. Analysis and Investigation of the Use Case

A popular misunderstanding regarding blockchain transactions is that they are completely anonymous. BTC is the most popular cryptocurrency blockchain and all its transactions are visible to the public. However, only transactional data are visible and no personal information linked to any of the transactions are available. The second most popular blockchain is Ethereum. In 2022, it was calculated that 80% of crypto theft involved the Ethereum blockchain. Due to no personal information being available to investigators, other techniques and

tools are needed to identify entities behind transactions. Five popular techniques are used when analysing and investigation a cryptocurrency crime (BIG Investigations, 2023):

3.1 Crypto Transaction Tracing

Transaction tracing is the primary technique and is also referred to as "follow the flow of funds". The process involves analysing transaction metadata such as the from and to addresses, the amount transacted and the timestamp to build a hypothesis. An investigator will try to identify hidden relationships, detect suspicious activities, and increase transparency.

3.2 Address Clustering

Address Clustering techniques involve the grouping of addresses that are likely to belong to the same person or entity within a cryptocurrency network. People often use a set of addresses for different transactions and tend to not create new addresses for each transaction. The technique considers the frequency, amount and timing of transactions. Several address clustering heuristics are in use today, see section 3.4 and Figure 7.

3.3 Graph Analysis

Graph analysis involves the visualisation of the flow of funds, making use of nodes to present the addresses and connecting lines to represent the transactions. This helps investigators to identify clusters, patterns, and other insights on the flow of funds. It also assists in understanding the relationships between various addresses and transactions. Crypto tracing, address clustering and graph analysis are often used in conjunction with each other, building a comprehensive picture of the flow of funds on the blockchain network.

3.4 Heuristics

Heuristics refers to using functions based on domain knowledge to enhance the performance of algorithms that find patterns leading to the identification of suspicious activities on a blockchain network. For address clustering, the multi-input-heuristic (MIH) method is the most effective and most studied one used today. It assumes that if two addresses (i.e. A and B), see Figure 7, are used as inputs with the same transaction, and one of the addresses is also used with another address (i.e. B and C) as inputs into another transaction, the three addresses A,B and C must be used by the same actor. The actor conducted both transactions and should be in possession of the private keys to all three addresses (Fröwis, 2020).

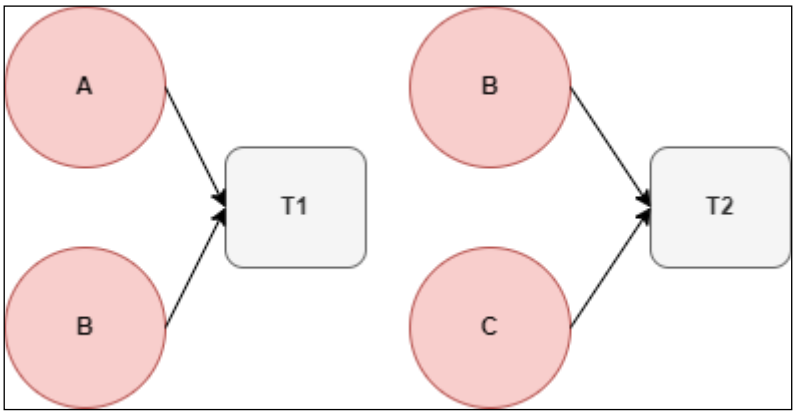

Figure 7: Multi-Input Clustering Heuristics (Fröwis, 2020)

3.5 Data Analysis

Data analysis involves the study of patterns, relationships and anomalies in the transaction information that could be key in closing complex cases. Good data analysis will uncover hidden relationships and patterns in large amounts of data and is key to cryptocurrency transaction investigations.

To perform cryptocurrency transaction analysis and investigations, a tool is needed that can assist in executing the five techniques mentioned above. A few tools exist such as Maltego, QLUE, Tatum, CipherTrace and

Breadcrumbs[3]. Most of the tools are quite expensive. However, Breadcrumbs has a more affordable option available and was selected for analysing and investigating the selected cryptocurrency giveaway scam.

The investigation has two angles to start off from:

1. The BTC contributing address (*scammer's BTC address*), **15YU4Pr3gDN78JjhgctKjRQ9NJhRdZn4Hf**, found on the landing page where participants can deposit funds into.
2. The ETH contributing address (*scammer's ETH address*), **0x766352635223f86abe5c970bb1c199df14099b8f,** also found on the landing page.

The first step was to enter the scammer's BTC address into the tool – it was discovered that no transaction took place. No funds have been received or sent from the address. This indicates that no scam took place on the BTC address. This could be due to the price of 1 BTC being too expensive, for targets and that they found it was cheaper to participate in the Ethereum giveaway. On entering the ETH address into the tool, the immediate results are that three transactions took place as incoming into the contributing ETH address, i.e. funds paid into the scammer's address. One transaction came from an address linked to the exchange Coinbase, one from a cryptocurrency wallet address and transactions from the exchange Binance (Figure 8). The final graph (after analysis had been done) is too big to be included in this paper as an image. The full graph can viewed at https://www.breadcrumbs.app/reports/9609 and a partial graph is provided in Figure 10. Note that Figure 7 is included in Figure 9, but in the latter graph, the resulting address nodes have been numbered from 1 to 4. The scammer's BTC address is shown in dark grey in Figure 9.

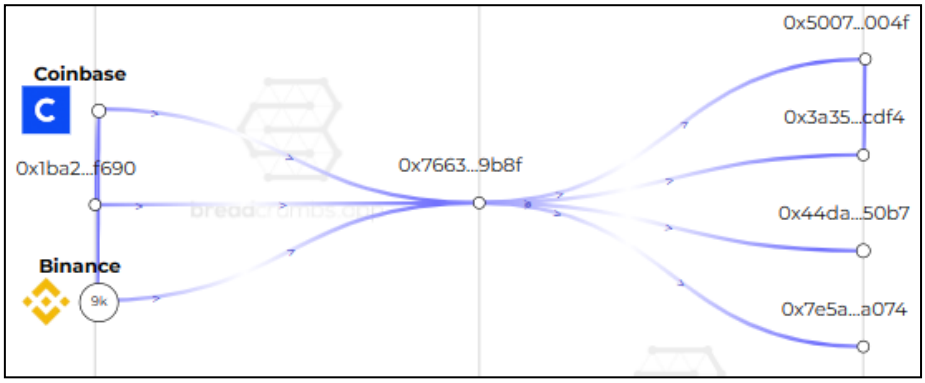

Figure 8: Scammer's ETH Address Incoming and Outgoing Transactions

Table 1 lists the direct incoming transactions from three sources into the scammer's address. Figure 9 indicates that a total of 2.3264 ETH has been sent to the scammer's address – this total corresponds to the sum of the amount ETH sent from the three sources. Note the first transaction into the scammer's address was done on 5 Jan 2024, indicating that this is a newly created address probably only for the lifetime of this scam. Also note the scammer's address still has a balance of 0.0039 ETH. Most of the incoming funds were moved quickly, with the last transaction executed on 8 Jan 2024.

Table 1: Direct Incoming Transactions into Scammer's Address

Source	From Address	Sent (ETH)	Timestamp
Coinbase	0xa9d1…3e43	1.1697	7 Jan 2024, 18:54
Wallet Address	0x1ba2…f690	0.9078	7 Jan 2024, 23:18
Binance	0x21a3…5549	0.2487	5 Jan 2024, 18:30

The main interest is to determine where the funds have been sent to from the scammer's address. Following the funds can become a daunting task and one must go through hundreds or thousands of transactions. The aim is to link the sent transactions to an exchange. Once this can be identified, an investigator can interact with law enforcement to issue a subpoena, instructing the exchange to reveal the personal information behind the address linked to their exchange.

[3] www.breadcrumbs.app

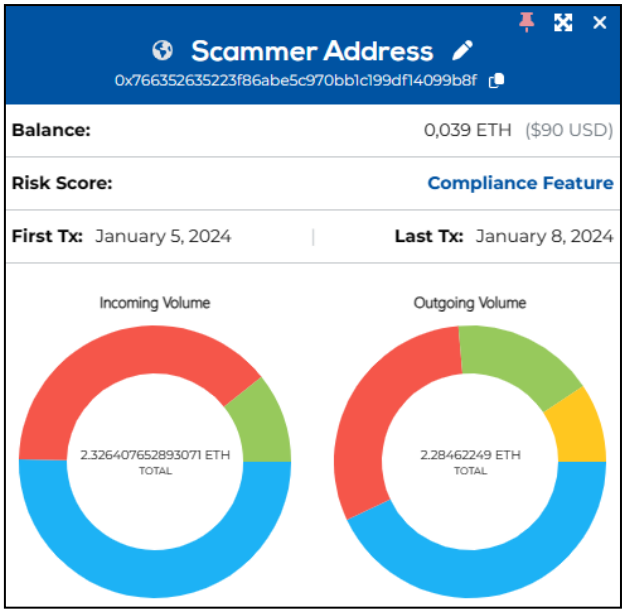

Figure 9: Scammer's ETH Incoming and Outgoing Volume

Four outgoing transactions were made to four cryptocurrency wallet addresses from the scammer's address, see Figure 8. Table 2 lists the four transactions' details at the time of writing. The amounts and number of transactions may be different in the future if funds have been moved in the interim.

Table 2: Direct Outgoing Transactions from Scammer's Address (Including the Total Received and Total Sent)

To Address	Received (ETH)	Timestamp	Total Received (ETH)	Total Sent (ETH)	Balance (ETH)
(1) 0x5007…004f	0.9825	7 Jan 2024, 23:37	0.9825	0.9814	0
(2) 0x3a35…cdf4	0.7	7 Jan 2024, 23:46	1.6814	1.6794	0
(3) 0x44da…50b7	0.3874	8 Jan 2024, 19:51	**38.7051**	**32.1114**	**6.527**
(4) 0x7e5a…a074	0.2146	8 Jan 2024, 20:38	2.3328	2.3019	0

In Figure 10, three incoming and four outgoing transactions are linked to the scammer's address. An interesting observation on the outgoing transaction from the address **(1) 0x5007…004f** is that the total amount of funds received from the scammer address was transferred to the address **(2) 0x3a35…cdf4**. The total amount sent out is slightly less than the total amount received, but the balance is 0. This discrepancy is due to transaction fees that are subtracted. The same applies for all the transactions, for each transaction there is a fee to be paid.

The total amount received in address **(2) 0x3a35…cdf4** was moved, leaving the balance at 0 ETH. By making use of Breadcrumb's functionality to follow the flow of funds, it was discovered that a transaction had been made into an exchange called FixedFloat. The two addresses (1 and 2) both have a balance of 0 ETH, indicating the funds have been moved out. Further tracing showed funds were moved into another address linked to FixedFloat, with a balance greater than 0. All addresses with a balance greater than 0 ETH will be marked as an address of interest, and indicated in light grey in Figure 10. Since the address is linked to an exchange, the next step is to determine if the exchange requires Know Your Customer (KYC) information. If this is the case, together with law enforcement agencies, a subpoena can be issued to the exchange to reveal the personal information linked to the addresses. With such personal information, the investigator can continue the investigation using traditional OSINT techniques. Contacting law enforcement to conduct a further investigation is out of the scope of this paper.

The address **(3) 0x44da…50b7** received 0.3874 ETH from the scammer's address and in total 38.7051 ETH were received *(at the time of writing)*. This indicates that funds were received from other addresses as well, possibly more scams were run, and that this address is used as a more permanent address into which to move funds from the scams. In other words, this address was probably not just used for the lifetime of the scam; it is likely one of the scammer's personal addresses where funds are transferred into from his various scams. This is

regarded to be a mistake made by the scammer and the address will be closely monitored. Future research can be done to follow the funds backwards, and possibly link the address to more scams. Links from other sources to this address is not covered in this paper, because hundreds of transactions have been found to be coming in to this address. Another observation is that only 32.1114 ETH has been sent out of this address, leaving the balance at 6.527 ETH. Since the balance is not 0, this address is marked as an address of interest and will be monitored until funds are being moved again. Breadcrumbs has the functionality to monitor certain addresses and to send notifications when funds are moving from the address. By following the flow of funds, Breadcrumbs indicated that hundreds of transactions have been linked to this address, in and out, further indicating that this is a permanent address being used by the scammer.

One of the outgoing transactions (out of address 3) is linked to an address, **0x2f1d…4d12,** from the exchange Kucoin. Kucoin requires KYC and steps can be taken to issue a subpoena to obtain personal information linked to the address and Kucoin account. Tracing funds from the Kucoin address, **0x2f1d…4d12**, shows a transfer has been main into a Kucoin Main Wallet address, **0xcad6…8fdd.** The latter address is shaded in light grey in Figure 9. Continuing the tracing, a transaction made from the FixedFloat address **0x4e5b…972f** into the same Kucoin Main Wallet address was detected (the FixedFloat address appears directly above the Kucoin address in Figure 9). This indicates the scammer is performing some sort of mixing, where he transfers funds to various addresses and exchanges and then eventually transfers all the amounts back to one specific address.

Another key finding is that transactions from the exchanges Coinbase and Binance are linked to this Kucoin Main Wallet address. Since many transactions point to the Kucoin Main Wallet address, it is being monitored and marked to be of high interest. This is a crucial result because an investigator can request a subpoena to be issued to all exchanges with known links to this wallet, and then compare current known personal information to the new information gathered from these exchanges. If the scammer is very advanced, he may be making use of mules and not be using his own personal information on the exchanges. However, it is a step in the right direction. If the sets of personal information from the various exchanges match, the probability that the target person can be identified is high.

Further tracing revealed that a transaction was made to the address **0xacc3…0x26** from the Kucoin Mani Wallet address. A transaction was also made into the same address from **(3) 0x44da…50b7** via one hop through the address **0x9f5d…c45f**. The address **0xacc3…0x26** is marked as high interest due to a large amount of ETH as the balance. From this address, **0xacc3…0x26**, things became more interesting; a number of transactions were made into various wallet addresses and into exchanges such as Binance, OKX, MXC and FixedFloat. The Binance address, **0x9b39…76fd** and the OKX address, **0x57ae…adb6** both had balances greater than 0 ETH, and is consequently marked as addresses of interest. Subpoenas to all the exchanges need to be issued to obtain personal information. From the latter address, two hops back of Figure 9, transactions were made into the exchanges HitBTC and WhiteBit. Again, subpoenas are to be issued to the exchanges as well. The address from WhiteBit, **0x4853…1e54,** had a very large amount of ETH linked to it and is marked as an address of high interest. Since the balance in this address is very high, it can be requested that a subpoena also includes a request to freeze this address to prevent any further transactions. Another finding is that various transactions were made from the Binance address, **0x9b39…76fd**, into multiple addresses also linked to Binance. From these Binance addresses, multiple transactions were made back into a previously used address linked to FixedFloat, **0x4e5b…972f.** Based on these patterns showing transactions back and forth between the same addresses, it can be said with high certainty that the addresses belong to the same scammer.

The address **(4) 0x7e5a…a074** received a total amount of 2.3328, but only 0.2146 has been received from the scammer's address. This is also an indication that this address can possibly be linked to more scams sending scammed funds to this address. By continuing to follow the flow of funds, it has been discovered that transactions were made into the address **0x24b5…2a25.** Another fund transfer to this (latter) address came from **(3) 0x44da…50b7**; this indicates that the address **0x24b5…2a25** is used as a more permanent address into which to transfer funds. A similar pattern of transfers was found for both the address **0x82e2…14ab** the address **0xae7a…fe84**. **0xae7a…fe84** is linked to the Bitget exchange and contains a very large amount of ETH. This address is marked of very high interest. Bitget could be issued with a subpoena to obtain personal information to identify the person of interest.

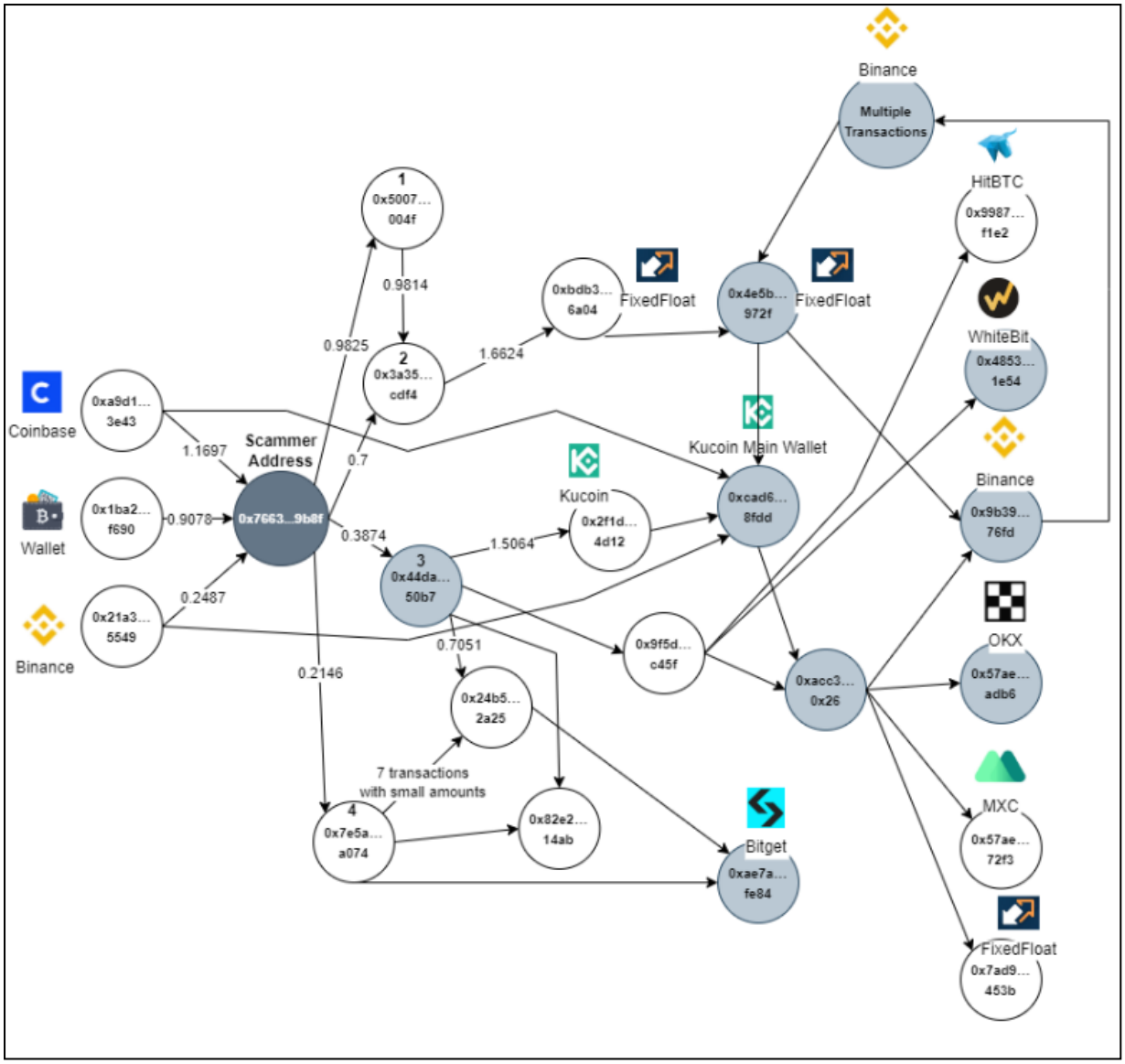

Figure 10: Transaction Tracing

It should be noted that none of the ETH addresses that were uncovered during this analysis did not match the visible parts of the addresses listed in Section 3, Figure 6. It can be confirmed that those addresses were fake generated addresses and not real addresses on the Ethereum blockchain.

4. Protection Against and Avoiding Giveaway Scams

Scammers are drawn to cryptocurrency for various reason such as there is no bank or centralised body to identify suspicious transactions and crypto transactions cannot be reversed. Various types of scams exist in the crypto space and a giveaway scam is one just one example of these (Agarwal, 2024). Giveaway scams are normally done by an impersonation of a legitimate platform or a celebrity as mentioned in in Section 1. It should be noted that legitimate platforms do run real promotions and giveaways, but they will never request a crypto amount to be sent in exchange for a larger return investment. No celebrity or famous influencer on social media platforms will send a direct message (DM) to any unknown individual to “help” with any trading or investment schemes. Users should not click on any link sent by someone that offers any cryptocurrency investment advice (Botha, Badenhorst, & Leenen, 2023).

Scammers are leveraging artificial intelligence (AI)-powered tools to amplify their reach and to create a fanbase of thousands of people on their social media accounts. The fake account interactions are used to give the illusion of popularity of their scam projects. They also make use of AI driven bots to engage with individuals providing

investment advice. A good example of how AI is used by scammers is by "pig butchering" scams. A bot can spend days to befriend someone on social media and to gain their trust just to end up scamming later. Fortunately, AI can also be used to protect individuals from giveaway scams. An AI system, called GiveawayScamHunter, has been developed by researchers from San Diego State University in the United States to detect and expose cryptocurrency giveaway scams on Twitter. The system has identified over 95, 000 scam lists that were created by over 87 000 accounts on social media platforms between June 2022 and June 2023. The team trained a natural language processing (NLP) tool on data from previously identified scams, which enabled them to identify close to 100 000 instances of giveaway scams. In addition, the system can extract the scam giveaway Internet domains and scam-related cryptocurrency wallet addresses. The system reported that 365 victims were attacked by cryptocurrency scams during this period and have suffered losses of over $872, 000 (Haqshanas, 2023).

Below is a check-list of some common red flags to protect against cryptocurrency giveaway scams (Hetler, 2023):

- A promise is given of very large gains or returns on investments.
- The only form of payment accepted is cryptocurrency.
- There will be no contractual obligations.
- Any form of communication, for example emails or social posts, contains spelling or grammar mistakes.
- Scammers always make use of manipulation tactics such as blackmail or extortion.
- Fake endorsements of influencers or celebrities will be found.
- Very few details will be provided about the investment and money movements.
- Several transactions are taking place in a day.

If an individual believes that he/she has been scammed, they should report it immediately. Scams can be reported at their country's Internet crime or complaints center or any federal trade commission or organization. If an exchange was linked to the scam, the exchange should be notified (Hetler, 2023). It can also be reported on chainabuse[4]. To avoid these types of scams, it is necessary is to understand that no-one on the Internet is going to give something away for free, and no one will double an investment amount in exchange for a payment in cryptocurrency coins. If it sounds too good to be true, it usually is. An investor should think twice before sending cryptocurrency funds; all transactions are irreversible, and it is not possible to get the funds back once it is sent (Bureau, 2022) (Hauer, 2020).

5. Conclusion

Blockchain adoption continues to increase and so do crypto-crimes and scams. This study provided examples of known crypto giveaway scams and raises awareness regarding these type of scams. A use case was selected from the data source chainabuse.com. The selected case is a crypto giveaway scam promoted via a manipulated YouTube Live Stream video of an interview with the former CEO of Microstrategy, Mr Michael Saylor. The video navigates participants to a webpage containing more details on the giveaway promotion (or rather the scam). Once a user participated by sending crypto to the specified address, they have been scammed. The paper indicates key pointers on how to investigate such a scam. The key pointers are put to practice with a blockchain analysis and investigation tool, Breadcrumbs, capable of tracing the flow of funds on the blockchain, perform address clustering, graph analysis, heuristics and data analysis. The analysis and investigation aim to trace the funds up to a point where a link can be made to a crypto exchange. Once a link can be made, in collaboration with law enforcement agencies, a subpoena can be issued to the exchange to instruct them to reveal the personal information linked to the address on their exchange as well as all transactional information. However, this is out of the scope of this paper and the analysis ends when a link can be made to an exchange. The study also aims to raise awareness of protective measures against these scams. Since there is no official legislation in place to guard against crypto scams, it remains a very significant international threat that cannot be ignored.

References

Agarwal, U. R. (2024). Blockchain and crypto forensics: Investigating crypto frauds. *34(2)*, p. p.e2255. International Journal of Network Management.

BIG Investigations. (2023, Mar 1). *The Must-Have Crypto Tracing Techniques For 2023*. Retrieved from Blockchain Intelligence Investigations (BIG): https://blockchaingroup.io/the-must-have-crypto-tracing-techniques-for-2023/

BitcoinAbuse.com. (2024, Jan 8). *Bitcoinabise.com*. Retrieved from Bitcoinabuse.com: https://www.bitcoinabuse.com/

[4] www.chainabuse.com

Botha, J., Badenhorst, D., & Leenen, L. (2023). An Analysis of Crypto Scams during the Covid-19 Pandemic: 2020-2022. *International Conference on Cyber Warfare and Security* (pp. 36-48). Towson University, Baltimore County, Maryland, USA: ACIL.

Bureau, C. (2022, May 18). *WORST Crypto Scams in 2022!! DONT Fall For These!!* Retrieved from YouTube: https://www.youtube.com/watch?v=GKTa5ciCJl4

Chainabuse.com. (2024a, Jan 8). *Chainabuse.com*. Retrieved from About: https://www.chainabuse.com/about

Chainabuse.com. (2024b, Jan 8). *Chainabuse.com*. Retrieved from Impersonation Scam: https://www.chainabuse.com/report/984f747b-ab29-4ae1-b127-6fc880ca4c45?context=browse-category&category=IMPERSONATION

Forbes. (2024, Jan 8). *Profile - Michael Saylor*. Retrieved from Forbes.com: https://www.forbes.com/profile/michael-saylor/?sh=556a1c557e0f

Fröwis, M. G. (2020). Safeguarding the evidential value of forensic cryptocurrency investigations. *Forensic Science International: Digital Investigation. 33*, p. p200902. ScienceDirect. Elsevier.

Guez, S. (2023, Mar 23). *Chatbots, Celebrities, and Victim Retargeting: Why Crypto Giveaway Scams Are Still So Successful*. Retrieved from akamai.com: https://www.akamai.com/blog/security-research/crypto-giveaway-scams-are-still-successful

Haqshanas, R. (2023, Aug 12). *Researchers Deploy AI to Uncover Crypto Giveaway Scam Schemes on Twitter*. Retrieved from Cryptonews.com: https://cryptonews.com/news/researchers-deploy-ai-uncover-crypto-giveaway-scam-schemes-twitter.htm

Hauer, T. (2020, April 6). *Crypto giveaway scams and how to spot them*. Retrieved from Coinbase: https://www.coinbase.com/blog/crypto-giveaway-scams-and-how-to-spot-them

Hetler, A. (2023, Dec 23). *11 common cryptocurrency scams in 2024*. Retrieved from TechTarget: https://www.techtarget.com/whatis/feature/Common-cryptocurrency-scams

Pelker, C. B. (2021). Using Blockchain Analysis from Investigation to Trial. *69*, p. p59. Dep't of Just. J. Fed. L. & Prac.

Random Generated Link 1. (2024, Jan 8). Retrieved from https://bafybeihmck427mca37tkz22zpceglcrzpmvxr67bbt75o6telnvyzkqmay.ipfs.w3s.link/v%3DPaSQ5dZ25dg.pdf

Random Generated Link 2. (2024, Jan 8). Retrieved from https://bafybeic2yumotbzu6u36tkteckdceqrftfyqyye4xegczin5iufuh7nmaq.ipfs.w3s.link/mstrx2.com.pdf

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