Analysis of a Cryptocurrency Investment Scam: Pig Butchering

Johnny Botha[1], Kreaan Singh[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
ksingh1@csir.co.za
lleenen@uwc.ac.za

Abstract: This paper analyses and investigates a cryptocurrency investment scam involving the suspicious and fraudulent cryptocurrency trading platform, Elite-Bit, through a detailed case study of a victim's experience. With the rapid rise of cryptocurrency, deceptive platforms like Elite-Bit exploit unsuspecting investors by presenting a façade of legitimacy. This case study chronicles the victim's journey, beginning with a seemingly romantic connection through a dating platform, to an introduction to an investment opportunity, and subsequently a financial loss. After investing a substantial amount, the victim faced unexpected barriers when attempting to withdraw funds, including exorbitant transaction fees and other fabricated costs. The analysis reveals how Elite-Bit employs manipulative tactics such as social engineering and false urgency to maintain control over investors, ultimately leading to significant financial loss. These manipulative tactics are referred to as pig butchering. The paper utilises qualitative data from interviews and correspondence with the victim, along with an examination of platform behaviours to highlight common patterns in cryptocurrency scams. An on-chain and off-chain analysis was conducted using the limited input data provided by the victim. To contextualise the collected information, a link analysis was done, utilising the tool Maltego. The link analysis visually maps the entities associated with the suspect within a network of nodes and connections. By situating the Elite-Bit case within the broader context of cryptocurrency regulation and consumer protection, this paper underscores the urgent need for enhanced regulatory frameworks and public awareness initiatives. This study aims to contribute to the ongoing discourse on financial fraud in the cryptocurrency sector, providing insights that may assist in the prevention of future scams and the promotion of more secure investment and trading practices.

Keywords: Chain analysis, Cryptocurrency crime, Investment crypto-scam, OSINT, Pig Butchering Crypto-scam, Romance crypto-scam

1. Introduction

The adoption of blockchain technology has surged in recent years. However, the unique characteristics of cryptocurrencies have also led to a rise in crime, drawing in scammers and fraudsters. The case analysed in this paper pertains to a fraudulent cryptocurrency investment and trading scam. The majority of frauds involving cryptocurrency trading or fake investments begin on social media or through messaging apps. It should be noted that unsolicited contact from an unknown individual or an online acquaintance introducing an unfamiliar trading platform significantly increases the likelihood of fraudulent activity (CTFC, 2025).

The case on which this paper is based started as a romance scam that escalated into a pig-butchering cryptocurrency investment fraud. Pig butchering scams are sophisticated and well-orchestrated in deceiving and defrauding victims. These scams mostly follow a pattern of **initiating contact** with a potential victim through a **fake persona**. The scammers will spend weeks, and sometimes months, building a relationship with the victim, often feigning a romantic interest. Once **trust** is gained, the scammer will direct the conversation towards **introducing investment opportunities**, usually involving cryptocurrency. The scammers will frame their scam as a very good opportunity to build a future together and achieve financial freedom. Scammers portray themselves as experienced investors or traders who want to help the victim to succeed. The scammer convinces the victim to install some investment app or to register on a fraudulent investment platform. This is followed by walking the victim through creating an account and the **initial deposit**. Normally a smaller amount is requested such that the victim is not intimidated. The scammer then uses manipulated data and fake reports to show high returns on the investment and encourages the victim to invest even higher amounts by creating an urgency of a once-in-a-lifetime opportunity. False profit reports will be shown to the victim and emotional **manipulation** tactics are used to stay in control, such as professing love, and promise of a shared future. The scammer could use threats and intimidation tactics causing the victim to panic if they do not act fast. When the scammer has extracted as much money as possible from the victim, they would cut all communication and **disappear**. The app or website is taken down if enough gains have been accrued. They could also keep the website alive if they want to move on to the next victim (Hayes, 2024).

2. Case Background

Figure 1 presents a summarised timeline of events that occurred between June 15, 2024 and July 31, 2024. On June 15, a female victim from the United Kingdom (UK) matched with a male suspect on Tinder, initiating a conversation on the platform. After a week of communication on Tinder, they exchanged mobile phone numbers, and their interactions transitioned to WhatsApp. Communication persisted for an additional three weeks, during which the victim expressed her intention to visit her sister in Australia. However, she mentioned the financial burden of the trip and her need to save up money. Seizing this opportunity, the suspect introduced her to the trading platform Elite-Bit (Elite-Bit, 2025), promising substantial returns and assuring her that she would quickly accumulate the necessary funds. The initial step involved registering an account with Elite-Bit (www.elite-bit.net), followed by transferring funds to the platform. Elite-Bit only accepted cryptocurrency deposits, so the victim was instructed to download MetaMask, a widely used cryptocurrency wallet, and the Crypto.com mobile application, a well-known cryptocurrency exchange, to facilitate the transactions.

After registering on Elite-Bit and installing the necessary applications on her phone, the victim transferred the initial funds from her Lloyds account to Revolut. Revolut is a British multinational neobank and fintech company that offers banking services to individuals and businesses (Revolut, 2025). Revolut also facilitates the conversion of fiat currency into cryptocurrency, providing users with a platform for digital asset transactions. Fiat currency, such as dollars or pounds, is a government-issued legal tender that lacks intrinsic value, unlike gold or silver. Its worth is derived from the public's trust in the authority that issues it (Wooldridge & Cambell, 2024). Revolut was used to purchase cryptocurrencies to be sent to Elite-Bit, but the victim was instructed to first send the funds to her Metamask wallet. Metamask is a software cryptocurrency wallet used to transact on the Ethereum (ETH) blockchain. This request to not transact directly from Revolut to Elite-Bit may have been done to circumvent Revolut withdrawal restrictions and analysis or to mask the actual destination of funds from Revolut. As an example, if Revolut analyses withdrawals and Elite-Bits' Binance wallet gets sanctioned, Revolut would prevent direct withdrawals to Elite-Bit, disrupting the scam.

Elite-Bit provided a chat service for platform navigation and trading assistance through which the victim was guided through her first trade. The victim "**won**" the trade, almost doubling her initial investment, and was then coerced into making additional deposits into Elite-Bit to facilitate larger and more frequent trades. Multiple payments were made to the platform, and the victim was guided through five additional "successful" trades. As a result, the victim's perceived account balance increased to 21,320 USD Tether (USDT). USDT, the symbol for Tether, is a stablecoin (cryptocurrency) pegged to and backed by fiat currencies such as the US dollar. It is issued by Tether, a subsidiary of iFinex, a Hong Kong-registered company (The Investopedia Team, 2024).

At this stage, the victim indicated she had no additional funds to invest and requested to withdraw the accumulated balance. To make communication difficult, Elite-Bit restricted contact to the chat service, with no telephone or email contact details provided. The victim was instructed, via the chat service, to provide a screenshot of the cryptocurrency address designated for the withdrawal. As part of the withdrawal process, the platform conducted a "**test**" transaction by sending a small amount of cryptocurrency to the provided address. Upon confirming receipt of this test transaction, the victim trusted that the full withdrawal would soon be processed. The victim requested to withdraw the funds to her Lloyds bank account in the UK. In response, the platform stated that withdrawals exceeding $20,000 required a tax payment of $1,980. Complying with this requirement, the victim transferred the tax amount to the platform using the cryptocurrency stablecoin USDT. Subsequently, the platform demanded an additional service charge of $2,880 before processing the withdrawal. The victim was informed that the funds would be reflected in her Lloyds bank account within 48 hours. However, after the stipulated time, no funds were received. The victim subsequently received an email from the platform, sent from a Gmail account, stating that the payment had been unsuccessful and inquiring whether an alternative destination for the funds could be provided. Seeking advice, the victim contacted her acquaintance from Tinder, who recommended requesting the funds be transferred to her Ethereum (ETH) address on MetaMask. Upon relaying this request to the platform, the victim was informed that an additional fee of $3,400 would be required to process the transaction.

Elite-Bit further took advantage of Revolut's daily withdrawal limit of $500 to create a situation where multiple payments over several days were required to cover the required fees. They further threatened her with late payment fees if she failed to pay by a certain date. The victim panicked and requested help from several friends to open accounts on Revolut in their names, which she would use to send additional $500 payments per day. One friend assisted while another refused, advising that the victim was being scammed. Despite help from the friend, the victim could still not make the full payment in time and was charged the late payment fee. A final

charge to convert USDT to ETH was then levied. At this point, the victim sought further assistance from her Tinder "friend," but began to question the situation, ultimately realising that she had been scammed. Further details regarding the dates and amounts of the transfers can be found in Figure 1.

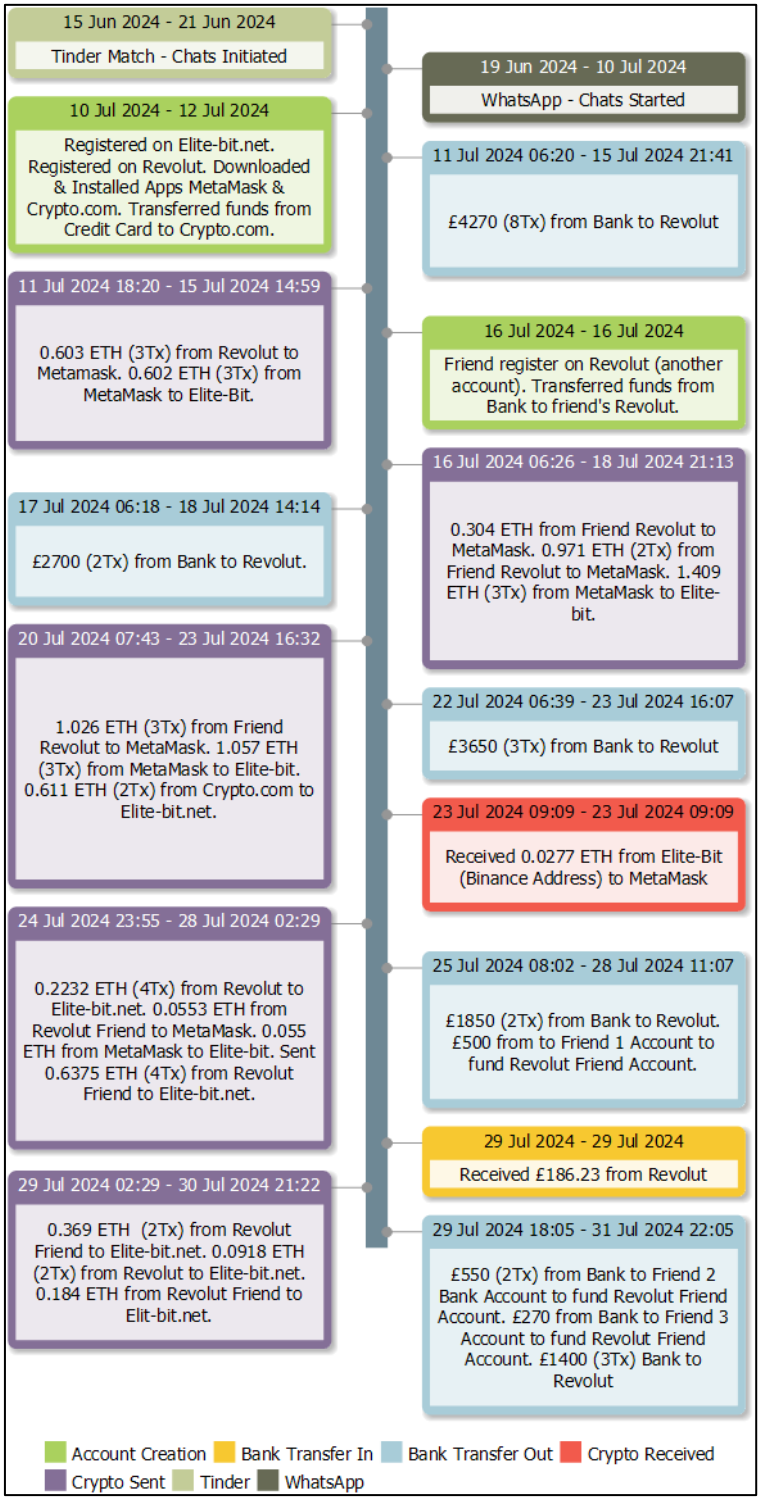

Figure 1: Summarised Timeline of Events (15 Jun 2024-31 Jul 2024)

A criminal case was opened in the UK and all legal proceedings will be conducted through the UK police. However, the victim was informed by the UK police that they would be unable to assist as the amount stolen was not substantial enough. The victim was advised that evidence of additional victims and larger losses would be required before the police would initiate an investigation. Subsequently, the victim sought the help of one of the authors of this paper, Johnny Botha, to assist in the analysis and investigation. Evidence indicating the

presence of additional victims was uncovered through blockchain analysis, though this aspect is not addressed within the scope of the current paper. This information could be shared with the UK police in the expectation that they would help from a legal perspective. Additionally, the victim may consider reaching out to other international law enforcement agencies, such as Interpol and Europol, to explore potential avenues for further support and cooperation in addressing the issue. The next section does a high-level evaluation of the website of the trading platform, Elite-Bit.

3. Evaluating the Trading Platform Elite-Bit

This section evaluates the platform Elite-Bit, highlighting several red flags and insights that an individual should be aware of. Elite-Bit claims to be a professional asset management and cryptocurrency trading platform. However, after a thorough evaluation, several red flags have been identified:

- Cryptocurrency prices are not updated in real-time as claimed.
- Certain web links and buttons are broken, giving a "404 page not found" error.
- The platform displays no credible business details.
- Price graphs lack tools that a professional trading platform would typically offer.
- Various time intervals are available for selection on the price graph, but selecting a time interval does not change the data displayed on the graph. Further inspection of the source of the code reveals that a JavaScript method is initiated upon timeframe selection, but it has no effect on the displayed information. The JavaScript source code could be obtained by right clicking in the browser and selecting the "View Source" option from the popup menu.
- A lack of access to a price history prevents the user from comparing or objecting to price action and trade outcomes.
- User actions are limited to betting on "high" or "low", akin to "buy" or "sell" actions on typical trading platforms.
- The list of trading transactions on the dashboard assimilates gambling and shows that the user has "**won**" X amount of USD or USDT. The first five trades were "**won**" and two remained in a pending status.

Open-source Intelligence (OSINT) is the gathering of information about an individual or organisation that is publicly available from sources such as websites, social media, and news articles. The information is unclassified, and intentionally discovered, discriminated, distilled, and disseminated for a specific audience and intelligence purposes (Steel, 2007). Additional investigation using internet search engines and OSINT techniques revealed the following red flags (CTFC, 2025). The platform or company:

- is registered in Estonia, but a USA address in Las Vegas and a USA phone number is displayed on the website.
- is not registered as a money service company, a requirement of any such service that operates in the UK.
- claims to have a license to trade forex, futures or options.
- claims to be registered with the Financial Conduct Authority (FCA), but upon inspection, it is using another company's details under a different name. This is referred to as a cloned firm.

Following discussions with the victim, several red flags were identified and highlighted (CTFC, 2025):

- The website only accepted cryptocurrency deposits. There are no bank transfer facilities.
- Investment returns increased substantially with increasing deposits – a possible manipulation tactic.
- When a withdrawal was requested, a large transaction fee was charged.
- After the transaction fee was paid, an additional fee for a tax clearance certificate was charged.
- An urgency was created to pay the service fees by giving a time limit. If funds were not received within the time limit, a penalty fee was charged.
- An unrealistically large service fee was charged for transferring ETH to the victim's MetaMask wallet.
- An unrealistically large service fee was charged for converting ETH to USDT.
- Email communication was sent from a free Gmail account, which is uncharacteristic of a professional service provider.

It should be noted that during the time of writing, the platform was still active until February 10, 2025, but now seems to be permanently offline. The next section covers the analysis done on the case with limited information provided from the victim as input.

4. Analysis of the Case

The methodology proposed by (Gertenbach, Botha, & Leenen, 2024) and subsequently extended by (Botha, Singh, & Leenen, 2025) serves as the foundation for the analysis presented herein. This methodology commences with the process of opening a case, which entails an initial investigation that integrates both on-chain and off-chain analyses. A parallel investigative path is then pursued, focusing on the on-chain aspect, with the objective of establishing a connection between each cryptocurrency address and corresponding social media accounts. Scammers often leverage social media platforms to advertise their fraudulent schemes. The final phase of the methodology involves a brief exploration of the legal frameworks and procedures necessary to transform actionable intelligence into evidence that is admissible in a court of law. The victim provided the following inputs *(redacted)*:

- ETH cryptocurrency address: 0x0f9f...54054
- Tinder Profile name: Fr…co Ab...e
- Mobile number: 4474…43
- Domain name: www.elite-bit.net (with login details)
- Gmail address: trade…net@gmail.com
- Bank statements of all transactions made to fund the platform Elite-Bit.

4.1 On-Chain Analysis

The tool Breadcrumbs (Breadcrumbs, 2023) was used to perform on-chain analysis. On-chain analysis is the way blockchain data is accessed and analysed by users. Typically analysing transaction history, wallet activity and smart contract interaction (TransFi, 2025) (Yang, Klages-Mundt, & Gudgeon, 2023).

4.1.1 Cryptocurrency address

The starting point of the analysis was the cryptocurrency address 0x0f9f…4054*,* provided by the victim and described as the address where she was instructed to deposit funds. Using Breadcrumbs selection tools to filter out transactions from several other victims, only this victim's deposits between 13-30 July 2024 *(the date range provided by the victim)* were investigated*.* Breadcrumbs identified the address used by Elite-Bit as an account held on the crypto exchange **Binance**. With such few transactions between the victim and the scammer, the investigation was simplified as it eliminated the need to check for money laundering techniques used to obfuscate and hide the scammer's intent. Binance can now be subpoenaed to instruct the exchange to reveal the account holder's personal information, as well as to provide the outgoing transactions made by the account holder.

Note*: Multiple incoming transactions to Elite-Bit's address outside of the provided date range have been identified. This indicates that the Elite-Bit address used for this victim is also used for other victims. This could provide additional insights from other victims but falls outside the scope of this study.*

The tool revealed several incoming transactions from four different sources (refer to Figure 2):

- MetaMask crypto wallet
- Revolut account of the victim
- Revolut account of a friend of the victim
- Crypto.com account

A total of 3.872 ETH was sent from the victim's MetaMask wallet to Elite-Bit. 0.4284 ETH was sent directly from the victim's Revolut account and 1.1915 ETH was sent from the friend's Revolut account. The total amount of ETH transferred added up to 5.4910 ETH.

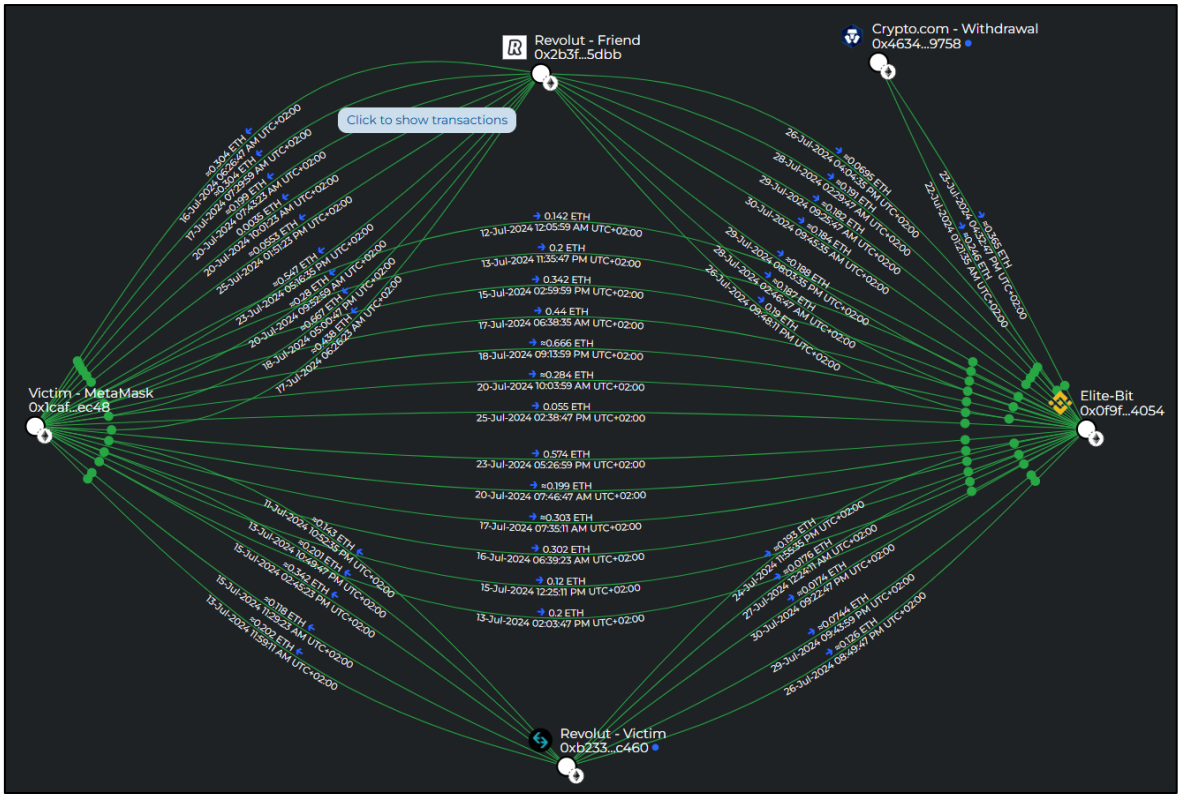

Figure 2: Incoming Transactions to Elite-Bit's Address

Analysing the Binance address of Elite-Bit (Figure 3), it can be seen the wallet is still being actively used *(at the* time of writing), with the last transaction dated 18 January 2025. This is despite the victim's last interaction with Elite-Bit in July 2024. This indicates that the scammers are still actively using their Binance account to scam other people. The total amount of cryptocurrency transacted through this address is 18.469 ETH, with 30% of the funds in this wallet originating from the victim of this study.

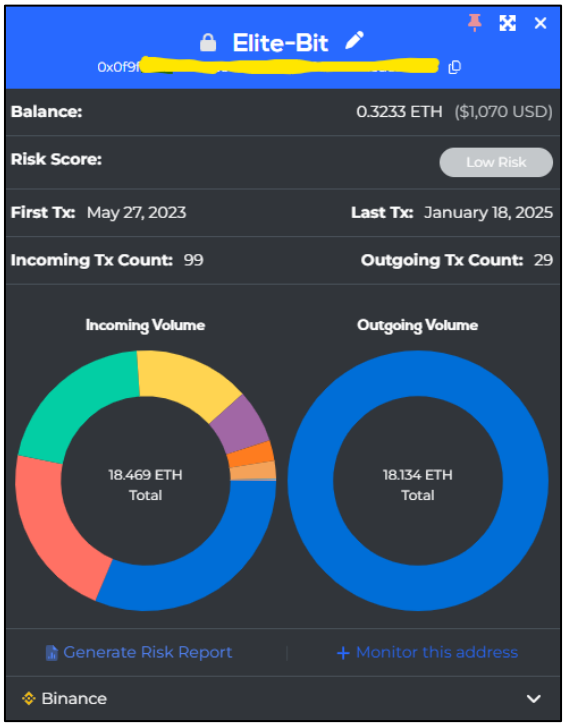

Figure 3: Elite-Bit - ETH Address

At the time of writing, a request has been made to the British High Commission in Pretoria, South Africa, to issue a subpoena to Binance. Since the case is not registered in South Africa, the subpoena must be issued by a UK law enforcement entity. No response has yet been received. Once the results of the subpoena are obtained, an off-chain analysis will be conducted utilising the personal information and outgoing transactions provided by Binance as a key point of reference. The following section presents the off-chain analysis, based on the inputs provided by the victim, excluding the subpoena information from Binance.

4.2 Off-Chain Analysis

This part of the analysis employs OSINT techniques in an attempt to unmask the identity of the suspect, given the information provided by the victim as outlined at the beginning of Section 4.

4.2.1 Tinder profile

Using tools such as TinEye (TinEye, 2025) and Google Image Search, it is possible to search the internet for the identity of a person in an image. An attempt to link the identity of the Tinder profile to the scammer was made using these tools, however, no positive results were returned. An alternative approach to identify the scammer could involve baiting the suspect by creating a shadow profile on Tinder that matches the characteristics of the suspect's typical victims, attempting to establish a match with the target. A VPN would be employed to manipulate the location to coincide with the suspect's last known country, city, and area. Once a match is made, Tinder displays the distance between the two profiles, enabling further search and location techniques. However, this approach falls outside the scope of the current study, and this route was not pursued. It must be noted that this approach often yields poor results, as the suspect could also employ the same technique of using a VPN to mask his/her real location.

4.2.2 Mobile number

According to data obtained from the mobile application Truecaller (Truecaller, 2025), the analysed mobile number has been identified as registered in the United Kingdom, remains active (at the time of writing), and is associated with the telecommunications service provider M-Hutchison. Standard OSINT techniques applied to the number of searches yielded no results. Law enforcement could issue a subpoena to uncover the personal information associated with the number through the service provider, though this action was not undertaken for this study.

4.2.3 Domain

Using the tool ViewDNS.info (ViewDNS.info, 2025), it was discovered that the domain is hosted in Kuala Lumpur, Malaysia. The domain name was registered on November 23, 2023, indicating that it is relatively new. This presents a red flag, as scammers often register new domains to facilitate fraudulent activities (Applegate, 2023). The IP address has been identified as 107.xxx.xx.26 (redacted). The registrar's information is protected, and obtaining this information would require issuing a subpoena to the service provider. The tool ScamAdvisor reported a trust score of 1/100, strongly indicating that the domain is linked to a scam. Additionally, by utilising the Scam-Detector tool (scam-detector.com, 2025), the registrar's name, address, country, and an additional phone number were revealed, identifying the suspect as Nigerian. This new information provided fresh insights and created a pivotal point in the investigation. The mobile app Truecaller (Truecaller, 2025) further revealed the name associated with the new number. Using these new inputs, OSINT techniques were employed to gather additional information online.

An additional finding is a license to trade number was found on the website. According to searches on the Financial Conduct Authority's (FCA) website (FCA, 2025), the trading license number used by Elite-bit belongs to another company. This is referred to as a cloned firm.

4.2.4 Gmail

The header file could not be obtained from the victim. This could have revealed the IP address where the email was sent from, and an approximate location could have been identified. Using OSINT techniques with the Gmail account, *trade…net@gmail.com,* a link was made to the domain name used and detected the account is linked to the scam Elite-Bit. No additional information could be obtained from the email account.

4.2.5 Bank statements and login details

By utilising the login credentials provided by the victim to access the website, transaction logs detailing deposits and trades were retrieved, as shown in Table 1. All payment transactions occurred between July 11, 2024 and

July 31, 2024. As indicated in Table 1 (Tx in the first column refers to transaction), the first two trades were refunded. According to discussions with the victim, the platform executed a trade, claimed that the market had turned against them, and subsequently refunded the amount to prevent financial loss. This strategy appeared to build trust with the victim. Following this, every subsequent trade resulted in the invested amount almost doubling in value.

Table 1: Elite-Bit - Transaction Log

Tx	Transacted	Amount	Post Balance	Detail
YC3TAVB8NKHB	2024-07-11 10:14 PM	+ 441.00 USD	441.00 USD	Deposits
7671R3AUAYEX	2024-07-12 07:12 PM	- 441.00 USD	0.00 USD	Trade to USDT High
7671R3AUAYEX	2024-07-12 07:49 PM	+ 441.00 USD	441.00 USD	Trade refund
9O6JKNUDJ75O	2024-07-12 08:03 PM	- 441.00 USD	0.00 USD	Trade to USDT High
737O8FYGK5FE	2024-07-12 08:41 PM	+ 441.00 USD	441.00 USD	Trade refund
PFFNZ4KAJYE3	2024-07-12 08:57 PM	- 441.00 USD	0.00 USD	Trade to USDT High
NR66A8EU2VQ4	2024-07-12 09:07 PM	+ 837.90 USD	837.90 USD	Trade to USDT WIN
PSDJBRUAA1N4	2024-07-13 12:15 PM	+ 627.00 USD	1,464.90 USD	Deposits
OXM616WYEKN8	2024-07-13 04:57 PM	- 1,464.00 USD	0.90 USD	Trade to USDT High
ZPUEK7T2MYCK	2024-07-13 05:17 PM	+ 2,781.60 USD	2,782.50 USD	Trade to USDT WIN
WB2MK5QZX5RH	2024-07-13 05:48 PM	- 2,782.00 USD	0.50 USD	Trade to USDT High
KUOSACS1B1XV	2024-07-13 06:05 PM	+ 5,285.80 USD	5,286.30 USD	Trade to USDT WIN
G2SKHK6NSUSX	2024-07-13 09:43 PM	+ 630.00 USD	5,916.30 USD	Deposit
G82WE22WMO4G	2024-07-13 10:24 PM	- 5,916.00 USD	0.30 USD	Trade to USDT High
6PYU111DAQMP	2024-07-13 10:41 PM	+ 11,240.40 USD	11,240.70 USD	Trade to USDT WIN
QNMV819XRUJ1	2024-07-14 09:52 AM	- 11,200.00 USD	40.70 USD	Trade to USDT High
29CVRQU7UY9S	2024-07-14 10:34 AM	+ 21,280.00 USD	21,320.70 USD	Trade to USDT WIN
5V9JUFQ68HN5	2024-07-14 09:36 PM	- 1,300.00 USD	20,020.70 USD	1,300.00 USD Withdraw Via BANK TRANSFER WITHDRAWAL METHOD
5V9JUFQ68HN5	2024-07-15 04:26 AM	+ 1,300.00 USD	21,320.70 USD	1,300.00 USD Refunded from withdrawal rejection
8P7FV7GO2491	2024-07-29 07:55 AM	+ 1,900.00 USD	23,220.70 USD	deposit

By July 14, 2024, a total of $1,698 had been deposited for trading purposes. The victim was led to believe that she had attained a trading balance of $21,320.70 and requested a withdrawal of her balance. Between July 15, 2024, and July 31, 2024, the scammer then employed pig butchering manipulation techniques to systematically exploit the victim of even more money. The victim's total payments amounted to £11,000 ($13,640.37), of which $11,942.37 was allocated to phantom service fees, tax fees, conversion fees, and penalty charges. Refer to Figure 1 for a detailed timeline of events, including all bank payments and cryptocurrency transactions.

4.3 Link Analysis

By employing OSINT techniques on the data provided by the victim, a substantial amount of relevant information was successfully gathered. When collecting information on a target, a case management strategy is needed to keep track and make sense of the findings. The 11P method (People, Places, Personalities, Places, Past, Police, Photos, Pay, Professional Life, Politics, Prejudice) from TCG Forensics (TCG Forensics, 2024) was applied to conduct profiling and link analysis on the suspect or target, as illustrated in Figure 4. Link analysis was applied using the tool Maltego, see Figure 4.

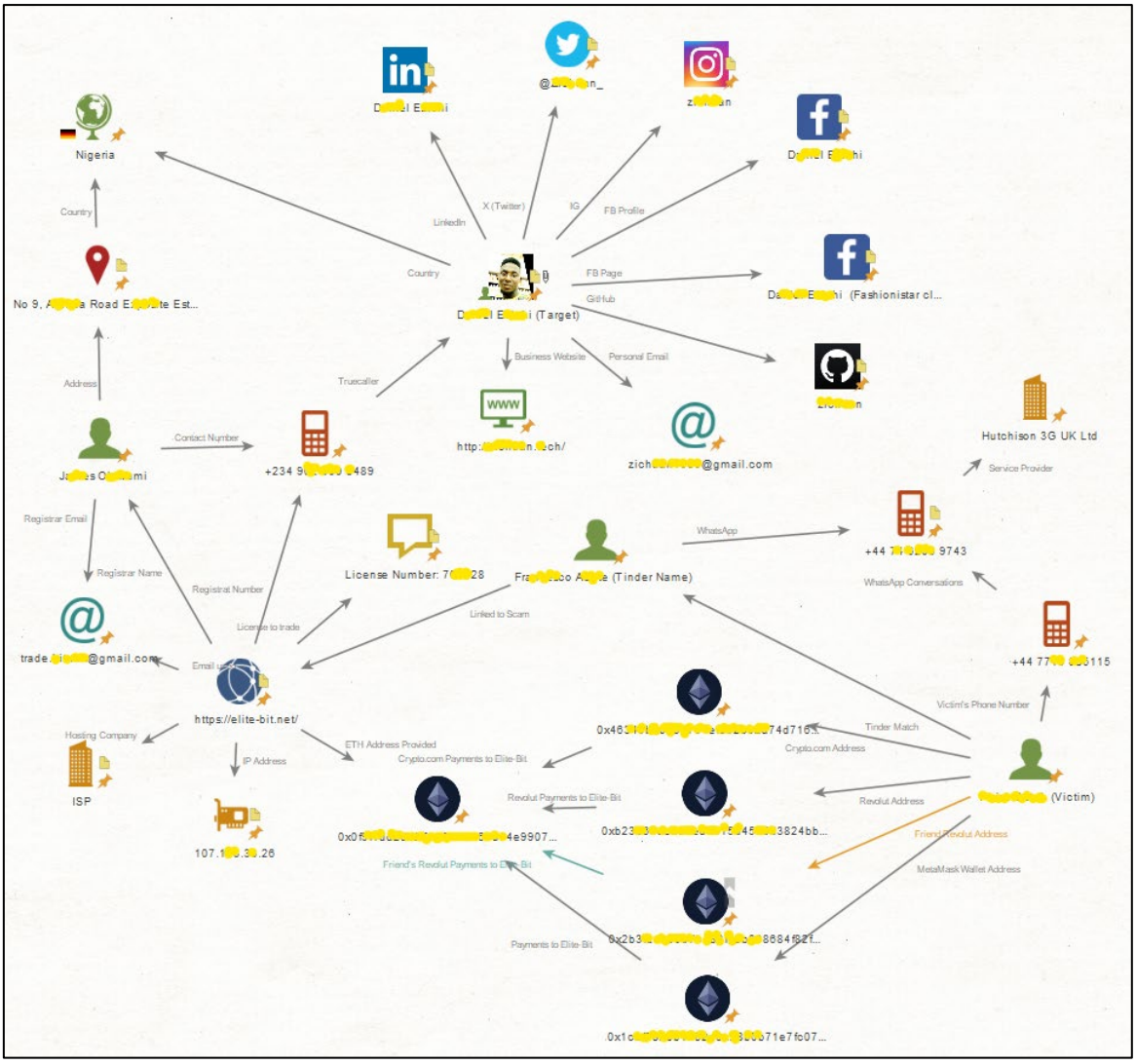

Figure 4: Link Analysis

Link analysis is employed to interpret the collected information by identifying relationships and connections within the dataset. This technique visually represents interconnected entities as nodes and links, facilitating a clearer understanding of the data and its underlying structure (Cambridge Intelligence, 2025). The link analysis enabled visual mapping of the connections between the victim and the suspect, including cryptocurrency transactions. Additionally, the analysis established links based on the collected information related to the domain name. The target's name and mobile number were retrieved from the domain registration details, and multiple social media associations were identified by applying Google Dorking techniques. These connections are illustrated in Figure 4.

4.4 Case Relevance

OSINT data has been gathered and may assist law enforcement in successfully identifying, arresting and prosecuting a suspect. Given the nature of this case originating on Tinder in the UK region, there is a high likelihood that other UK women are actively being targeted by the same scammer. It is therefore advised that

UK law enforcement consider the on-chain analysis and OSINT gathered in this paper to assist this and other victims as soon as possible. Doing so may reveal a ring of linked criminals that focus on crimes of this nature.

5. Conclusion

As blockchain adoption grows, the rise in cryptocurrency-related crimes and scams follows suit. This paper analysed a romance scam to systematically extract money from a victim in what the victim thought was a successful cryptocurrency investment. The romance scam therefore escalated into a pig butchering scam. The paper provides the case background and evaluates the fake investment platform Elite-Bit. The analysis of the case followed the methodology proposed in a previous study conducted by the researchers (Gertenbach, Botha, & Leenen, 2024) and (Botha, Singh, & Leenen, 2025). On completion of the on-chain analysis, an off-chain analysis using OSINT investigative techniques and methods was followed. The inputs to perform the off-chain analysis and OSINT techniques were a Tinder profile, mobile number, domain name, the transaction log on Elite-bit's website and bank statements from the victim. Lastly, a link analysis was performed on the suspect or target person, connecting online entities linked to the target.

Online scams remain a significant international threat due to the lack of standardised and official legislation. Furthermore, due to the borderless nature of cryptocurrency transactions, these scams are becoming ever more prevalent in financial and cyber crimes. This paper has been written to raise awareness around romance scams, fake crypto investment scams, and pig butchering scams. The case is actively being investigated by the CSIR in connection with UK law enforcement.

References

Applegate, A. (2023, Dec 21). *The Risks and Dangers of New Domains*. Retrieved from DNS Filter: https://www.dnsfilter.com/blog/risks-and-dangers-of-new-domains

Botha, J., Singh, K., & Leenen, L. (2025, Feb 3). A Proposed Bitcoin Blockchain Investigation Methodology: Based on a Case Study Approach. *Journal of Information Warfare, 24*(1), 1-18. Retrieved Feb 10, 2025, from https://www.jinfowar.com/journal/volume-24-issue-1/proposed-bitcoin-blockchain-investigation-methodology-based-case-study-approach

Breadcrumbs. (2023, Oct 11). *Breadcrumbs Investigation*. Retrieved from https://www.breadcrumbs.app/: https://www.breadcrumbs.app/home

Cambridge Intelligence. (2025, Feb 10). *Link analysis*. Retrieved from www.cambridge-intelligence.com: https://cambridge-intelligence.com/why-link-analysis/

CTFC. (2025, Jan 08). *10 Signs of a Scam Crypto or Forex Trading Website*. Retrieved from ctfc.gov: https://www.cftc.gov/sites/default/files/2023-04/SpotFraudSites.pdf

Elite-Bit. (2025, Jan 08). *Home Page*. Retrieved from elite-bit.net: https://elite-bit.net/

Gertenbach, W., Botha, J., & Leenen, L. (2024). A Proposed High-Level Methodology on How OSINT is applied in Blockchain Investigations. *19th International Conference on Cyber Warfare and Security* (pp. 75-83). Johannesburg, South Africa: Academic Conferences International Limited.

Hayes, A. (2024, Mar 26). *Pig Butchering Scams: What They Are, Warning Signs, and How to Avoid Them*. Retrieved from Investopedia.com: https://www.investopedia.com/pig-butchering-scams-8605501

Revolut. (2025, Feb 10). *Home Page*. Retrieved from www.revolut.com: https://www.revolut.com/

scam-detector.com. (2025, Feb 10). *Scam Detector Validator*. Retrieved from scam-detector.com: https://www.scam-detector.com/validator/elite-bit-com-review/

Steel, R. (2007). Open source intelligence. In L. Johnson, *Handbook of Intelligence Studies.* New York, USA: Routledge.

TCG Forensics. (2024, May 2). *Home Page*. Retrieved Jun 13, 2024, from TCG Forensics: https://tcgforensics.co.za/

The Investopedia Team. (2024, Mar 10). *Tether (USDT): Meaning and Uses for Tethering Crypto*. Retrieved from investopedia.com: https://www.investopedia.com/terms/t/tether-usdt.asp

TinEye. (2025, Feb 7). *Home Page*. Retrieved from TinEye: https://tineye.com/

TransFi. (2025, Feb 13). *What is On-Chain Analysis in Blockchain and How Do You Use It?* Retrieved from www.transfi.com: https://www.transfi.com/blog/on-chain-analysis-in-blockchain

Truecaller. (2025, Feb 10). *Number Search Results Page*. Retrieved from www.truecaller.com: https://www.truecaller.com/

ViewDNS.info. (2025, Feb 7). *Home Page*. Retrieved from ViewDNS.info: https://viewdns.info/

Wooldridge, L., & Cambell, T. (2024, Jun 20). *Fiat Money: Definition, History, and How it Works*. Retrieved from Business Insider: https://www.businessinsider.com/personal-finance/investing/fiat-money

Yang, Z., Klages-Mundt, A., & Gudgeon, L. (2023). Oracle Counterpoint: Relationships between On-chain and Off-chain Market Data. *arxiv*. Retrieved from https://arxiv.org/abs/2303.16331