Evaluating an Investigative Process for Cryptocurrency-Related Crimes

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 evaluates a previously proposed investigative process for cryptocurrency-related crimes, originally introduced by the authors (Botha, Singh, & Leenen, 2025a), through the application of a real-world case study. The process covers crime reporting and case registration, on-chain analysis, off-chain analysis, and the transformation of investigative intelligence into court-admissible evidence. The current study focuses on a new, active case involving an elderly South African (SA) woman who was defrauded of a substantial portion of her pension through a fraudulent investment scheme known as ###-Platform (redacted). The case is presently under investigation by the Directorate for Priority Crime Investigation (DPCI), a specialised unit of the South African Police Services (SAPS) tasked with addressing serious economic crimes and commonly referred to as the Hawks. By systematically applying the proposed investigative process to this case, the study assesses the framework's practical utility, adaptability, and effectiveness in real-world conditions. The analysis further reflects on legal, technical, and procedural challenges encountered during the investigation, offering critical insights for law enforcement, regulators, and cybersecurity professionals. It also highlights broader systemic vulnerabilities that facilitate such scams, particularly among elderly and non-technical populations. The findings underscore the need for enhanced public education, improved regulatory oversight, and international cooperation in combating cryptocurrency fraud. Ultimately, the paper contributes to the evolving discourse on financial crime in the digital age and aims to support the development of more secure and accountable crypto-investment environments.

Keywords: Blockchain, Chain analysis, Cryptocurrency crime, Investment crypto-scam, OSINT

1. Introduction

The adoption of blockchain technology has surged in recent years, and with it, a rise in criminal activity whereby fraudsters and organised crime use the complexities of blockchains to mask their activities. This paper analyses a fraudulent cryptocurrency investment and trading scam by using a investigate process proposed in previous publications (Botha, Singh, & Leenen, 2025a). Cryptocurrency trading or investment scams typically 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).

This paper examines a case centered around a fraudulent investment platform called ###-Platform. The platform's website is currently inactive. The paper includes background details provided by the victim related to this case. DPCI, also known as the Hawks, in SA, is leading the investigation. The case adheres to the phases and steps outlined in the proposed methodology detailed in the journal article: 'A Proposed Bitcoin Blockchain Investigation Methodology: Based on a Case Study Approach' by (Botha, Singh, & Leenen, 2025a). Initially, the study presents the case study background, followed by an analysis of the case on and off the blockchain, according to the proposed process steps. Once sufficient intelligence is gathered for profiling the target entity, a link analysis is conducted. The final step involves law enforcement procedures. The study aims to assess or evaluate the process through a case study approach. Feedback on the process is provided, discussing its strengths, weaknesses, and potential improvements. The final section concludes the paper's findings.

2. Case Background

An elderly woman contacted one of the authors, J Botha, to assist in the investigation and analysis of a fraudulent case in which she fell victim to. The victim was persuaded to invest in ###-Platform, which was portrayed to be a global online trading entity based in the United Kingdom (UK), integrating traditional investments with crypto-based funding and trading mechanisms. The platform promised to manage elderly victims' pensions and to generate large profits from the proceeds. The company advertised leveraged trading across various assets, including Bitcoin (BTC), Ethereum (ETH), the S&P 500, and Tesla, amongst others. ###-Platform asserted that their company had experienced significant growth, served international clients, and accessed top-tier liquidity

and a diverse array of trading tools while ensuring security to facilitate a safe and efficient trading environment for all participants (Trustpilot, 2023).

In March 2023, a criminal case was opened and assigned to a law enforcement officer from DPCI to conduct the investigation. The first author, J Botha, interacted with the official investigator to gather all necessary information for assistance. The victim had opened an account with VALR, a cryptocurrency exchange based in SA. It is important to note that VALR has no connection to ###-Platform. The victim went through customer onboarding, providing all necessary Know Your Customer (KYC) documentation and bank statements as required by VALR. She was granted an account, but while depositing money to VALR, VALR identified unusual deposit patterns considering the customer's risk profile and age. Upon inquiry, the customer assured VALR that she was not receiving assistance from anyone to perform these deposits, was not being scammed and thus requested proper allocation of the deposits. This attestation was accepted by VALR and the victims deposit of SA Rands (ZAR) were unrestricted. She acquired cryptocurrency and transferred her funds to ###-Platform. Once the victim realised that she was being defrauded, her responses to the prior questions changed significantly. She informed VALR of her use of ###-Platform and the substantial returns that were promised. Additionally, the victim revealed that the scammers had accessed her personal computer through the AnyDesk software application. AnyDesk is a remote desktop application that allows someone to take control over if permission is granted (AnyDesk, 2025). According to the victim, the scammers purportedly executed trades on her behalf on ###-Platform, as she was unfamiliar with the procedure.

The victim supplied the cryptocurrency address used in VALR from where the transactions were executed. She claimed to have lost close to ZAR4,950,000 (US $281,312) over two years. The claims correspond to the bank statements provided by the victim, showing deposits made into VALR from her bank account. It also corresponds with the police statement.

3. Analysis of the Case

The investigative process previously proposed by (Botha, Singh, & Leenen, 2025a) serves as the foundation for the analysis presented in this paper. The process has five phases, namely:

- Data collection
- Analysis
- Theory development and validation
- Suspect identification and reasonable grounds
- Legal action

The investigative process is depicted in Figure 1. For the full details of the process and steps, refer to the journal paper (Botha, Singh, & Leenen, 2025a). The analysis of the case study in this paper, follows this process and its proposed steps, which is outlined in the next sections with comprehensive explanations of each step with the case information provided as input.

3.1 Opening of Case

The opening of a case forms part of the data collection phase. In this particular use case, an investigation is already underway. Therefore, the first step to open a case has already been done. The victim has provided a BTC cryptocurrency address that was linked to the crypto exchange VALR in SA. Furthermore, a compilation of names and phone numbers of suspect individuals who contacted the victim and eventually defrauded her are also available. The victim provided the following inputs *(redacted)*:

- VALR transaction History File with a number of addresses and transactions. The two main in this file addresses were:
- *32jC##…QaYG*
- *1Lac##…XFpU*
- Web domain
- *www.###-platform.io*
- Names
- *List of names of people communicating over WhatsApp and Phone calls (multiple people and name – probably all fake names)*
- Phone Numbers
- *List of numbers that were calling the victim (SA and UK numbers)*

- Email Addresses
- *s#####e@cryptodotcom.info*
- *List of scammer names@###-platform.io*
- Physical Address
- *# B### St, London E## #BG, UK*

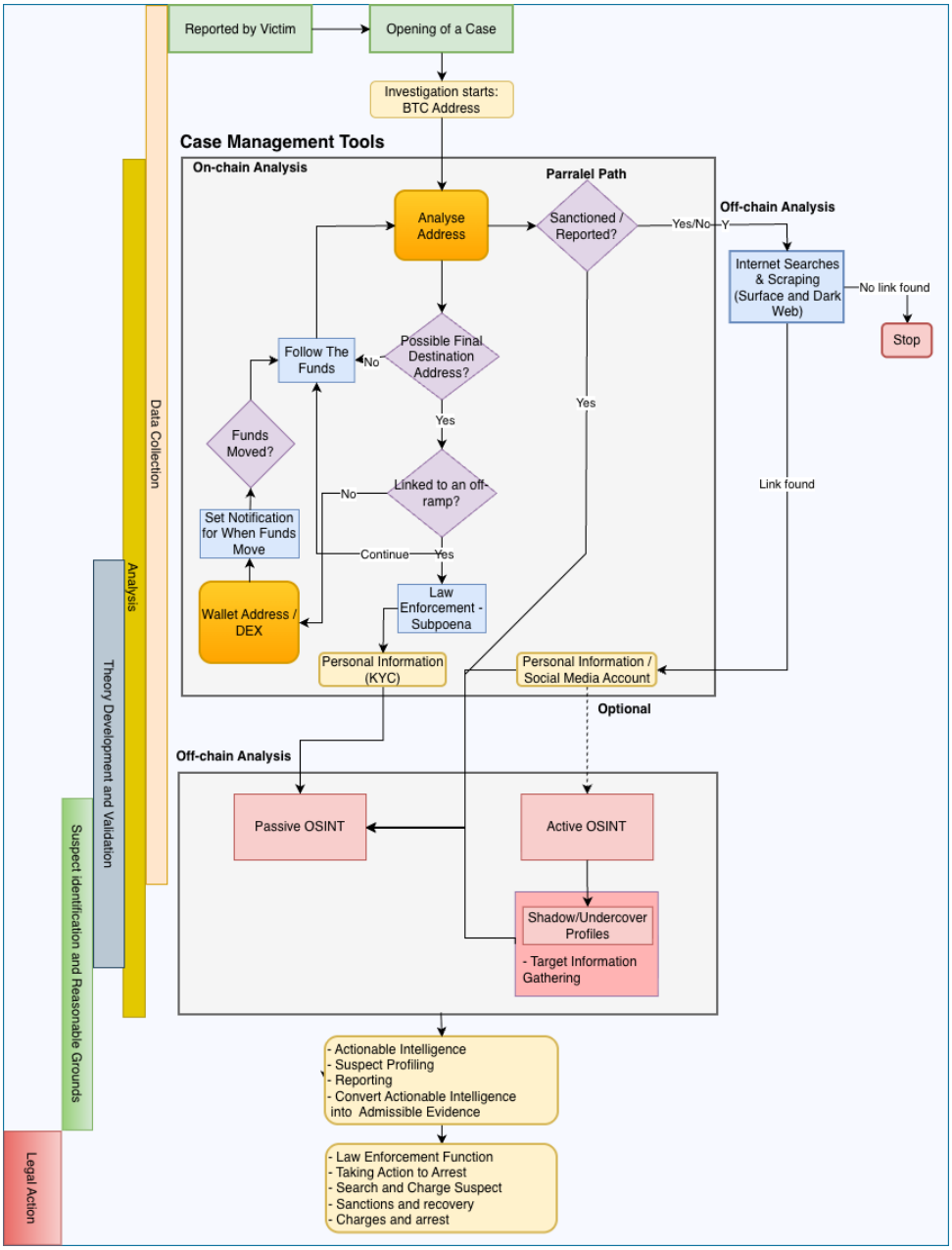

Figure 1: Process for Conducting Cryptocurrency Crime Investigations (Botha, Singh, & Leenen, 2025a)

3.2 On-chain Analysis

The on-chain analysis is primarily conducted during the analysis phase, but it also intersects with the data collection as well as the theory development and validation phases (refer to Figure 1). As the investigation advances, additional data is gathered, and new theories are continually developed and validated. The blockchain analysis tool known as Breadcrumbs (Breadcrumbs, 2023) was used to perform the on-chain analysis. This type of analysis examines blockchain data, focusing on transaction history, wallet activities, and smart contract interactions between users (TransFi, 2025) (Yang, Klages-Mundt, & Gudgeon, 2023). The analysis of this particular case began with the victim's two cryptocurrency addresses found in the transaction history file. The file contained crypto transactions, and detailed payments made to VALR that were converted into BTC from the victim's account. The address 32jC##…QaYG found in the file is the victim's BTC receiving address. There was

also one outgoing transaction from the victim's BTC address 32jC##…QaYG to a crypto BTC wallet address 1Lac##…FXpU. Because the victim's address was associated with VALR, the tool couldn't track outgoing transactions from the exchange. Blockchain analysis tools cannot follow the funds through a centralised exchange (CEX) because the exchange has internal transactions that occurs off-chain within its private internal ledger, not on the public blockchain. This breaks the public traceability (Chainalysis.com, 2020). However, with law enforcement's help, a section 205 subpoena was issued to VALR, leading them to disclose the outgoing transactions to the scammer's addresses. A section 205 subpoena is a legal tool under the SA Criminal Procedure Act that allows authorities to compel individuals or entities to provide evidence of information relevant to a criminal investigation. This includes ordering a third party, like a cryptocurrency exchange in this case, to disclose information and records (The Banking Association Aouth Africa, 2024). It was discovered that the scammers transferred the stolen cryptocurrency to three different addresses (see Table 1) including the reference names for each scammer address used in this paper.

Table 1: Scammer Addresses

Scammer Address	Reference Name in Paper
1End##…4EFo (which still holds 1.14 BTC)	Scammer-Address-1
142T##…xmGo (0.28 BTC)	Scammer-Address-2
1NvB##…gHfD (12.8 BTC)	Scammer-Address-3

VALR also provided a list of outgoing transactions from the scammer's addresses that linked to multiple cryptocurrency exchanges outside of SA. These transactions, addresses and linked exchanges are illustrated in Table 2. The flow of these transactions is shown in Figure 3.

Table 2: Outgoing Transactions from Scammer Addresses

TX	Address	Exchange
Bctq##…9zwn	32Eq##…ubrF	Coinpayments.net
bc1q##…qd0t	33jD##…Jen2	Kyrrex.com
bc1q##…xvw5	3Q7h##…izCB	Kyrrex.com
bc1q##…4eea	3AXC##…3Gvh	Kyrrex.com
bc1q##…jsnw	31ik##…8a6J	Kyrrex.com
bc1g##…4vm3	3HG7##…xRRu	Kyrrex.com
bc1g##…dmgy	33jD##…Jen2	Kyrrex.com

Another discovery was an additional VALR address, 39F4##…jVDX, linked to Scammer Address 3. Intelligence gathered from VALR led to the disclosure of the name and surname behind the address. This address was found to be the actual address belonging to the victim. The name behind the address found in the transaction history file, was the name of her daughter's former boyfriend who, according to the victim, was the one who introduced her to the investment platform. The victim stated that the former boyfriend had also fallen victim to the fraudulent platform, however he has not opened a criminal case to investigate the matter. More research is needed to accurately determine the ex-boyfriend's role and link to the victim and scammers addresses. In this paper, the victim's actual address will be referred to as 'Victim-Address-1' and the address of the former boyfriend as 'Victim-Address-2'.

Figure 2 illustrates the transaction flow originating from Victim-Address-2, the address of the former boyfriend of the victim's daughter and the victim's address, Victim-Address-1, into to the three scammer addresses. Three transaction flows will be discussed here, for each one of the scammer cryptocurrency addresses from the list above, to several cryptocurrency exchanges, based on the information obtained from the section 205 subpoena on VALR. The three scammer addresses are shown on the right side of Figure 2, inside the rectangle.

3.2.1 Scammer-Address-1

No direct transaction was identified with Scammer-Address-1. However, the funds were transferred from VALR, Victim Address 1, to a deposit address, 1LvG##…7Xpi, on Binance exchange, the largest cryptocurrency exchange globally. A section 205 subpoena was requested on this address to obtain the account holder details. However, no results have been obtained yet, at the time of writing. From Binance, the funds moved to an external wallet, bv1q2h…edux. Afterward, the funds travelled through seven transactions and cryptocurrency wallet addresses

to reach Scammer-Address-1, which currently still holds 1.14 BTC. This address is marked as a destination address, since no further transactions took place. A monitoring notification was placed using the tool Breadcrumbs, to notify the analyst via email or SMS when the funds are on the move again. If the address is proven to be linked to criminal proceeds, the address should be reported to sanctioning bodies, but, as an interim measure, it has been reported on chainabuse.com.

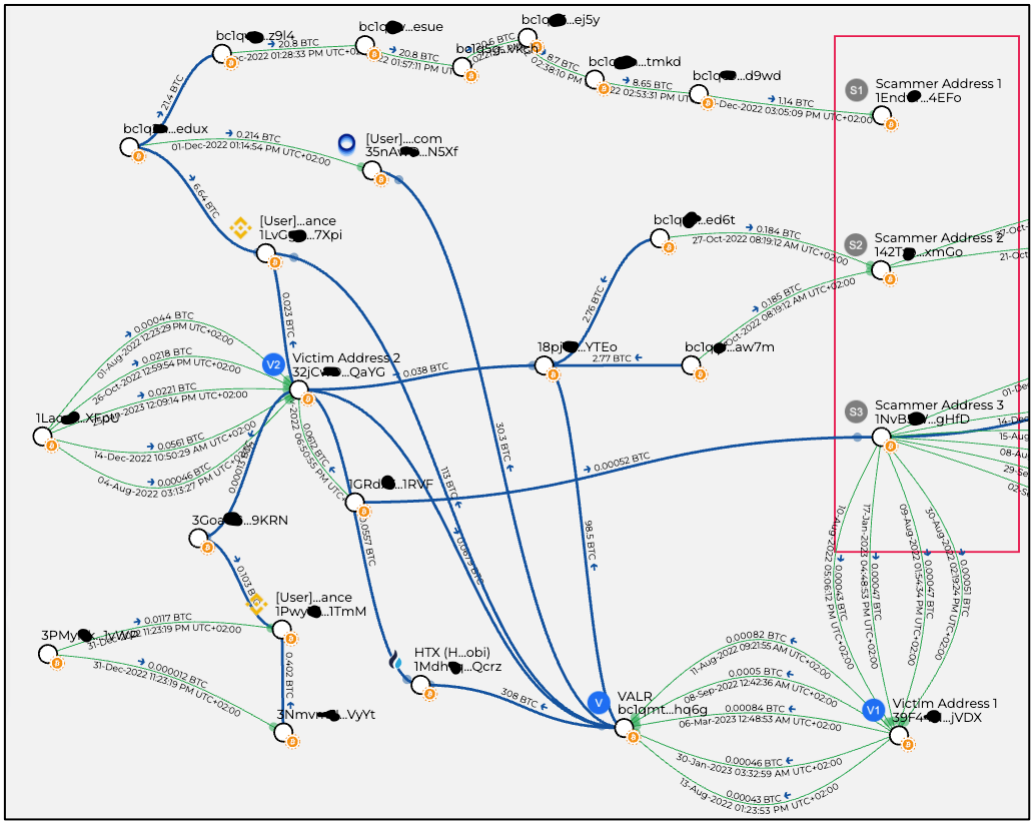

Figure 2: Outgoing Transactions from Victim Addresses to Scammer Addresses

3.2.2 Scammer-Address-2

Funds were transferred into Scammer-Address-2, see Figure 2 (middle right side of the figure) and Figure 3 (top left of the figure) through another wallet address as well as via the exchange HTX, also known as Huobi (HTX, 2025). From Scammer-Address-2, funds were transferred into two cryptocurrency wallet addresses, bc1q##…qqdd and bc1q##…fg8l, as illustrated in Figure 3 (top left and top middle side of the figure). Subsequently, these funds were moved to the exchange kyrrex.com, arriving at the address 3AXC##…3Gvh (top right side of Figure). The address in question is designated as a final destination due to the inability to track funds further. Nonetheless, according to trustworthy intelligence, 30,655.78 USDT was withdrawn from the exchange kyrrex.com into the external address TGXF##…MEVb, associated with the Tron blockchain. From this point, the funds were moved to other external Tron crypto addresses, including a transaction to a Binance address, see Figure 4. A section 205 subpoena is necessary to acquire details about the account holder and outgoing transactions from Binance. As for the additional crypto wallet addresses, further tracing of funds will be done to identify more destination addresses and exchanges.

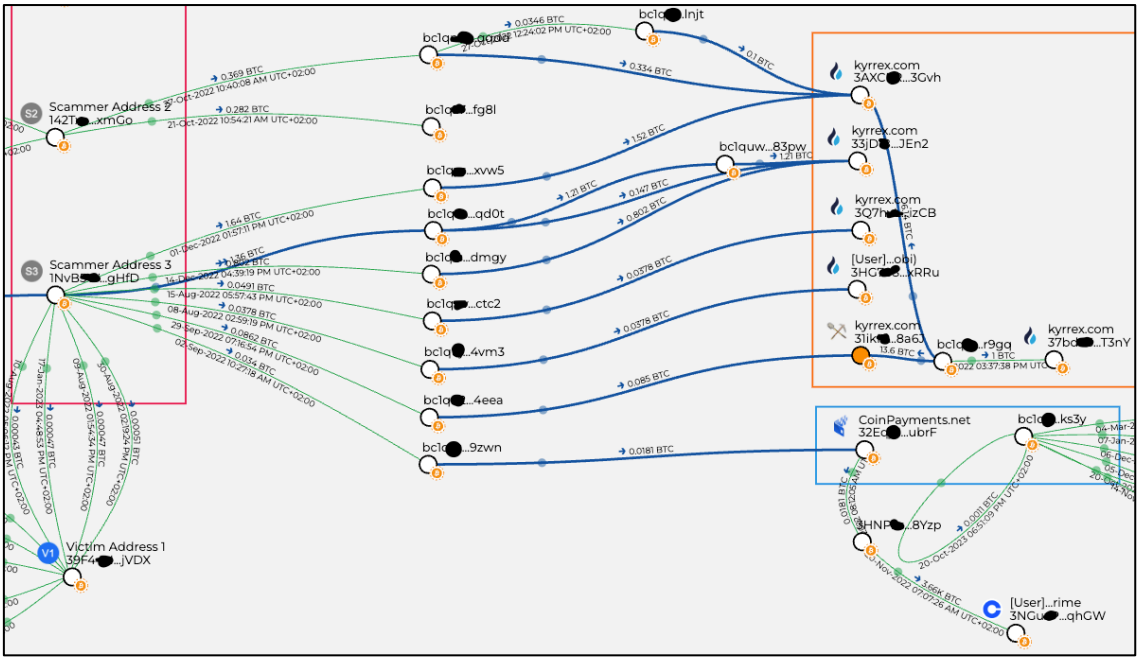

Figure 3: Outgoing Transactions from Scammer's Addresses to Cryptocurrency Exchanges

3.2.3 Scammer-Address-3

From the section 205 subpoena results received on VALR, a number of transactions flowed out of Scammer-Address-3 into the exchange kyrrex.com. These addresses can be seen in Figure 4 on the left side, inside the square. The Breadcrumbs tool flagged the address 31ik##…8a6J as a high-risk address (marked with a darker dot on the address node at the bottom left in Figure 4 and can also be seen in Figure 3, middle right inside the rectangle), meaning it has been linked to scams before. A section 205 subpoena is necessary to obtain further outgoing transactions and information on the account holder. Until this is issued, no further tracing can be performed. However, reliable information for Scammer-Address-3 (refer to Figure 3) also included a list of transactions out of these kyrrexx.com addresses to external addresses. Funds were converted from BTC into USDT on the Tron blockchain, and transferred to two Tron addresses, refer to Figure 4 (on the right).

Still following the path from Scammer-Address-3, based on the information from the VALR section 205 subpoena, transactions were made into the exchange CoinPayments.net (refer to Figure 3). The Breadcrumbs tool revealed that payments were made from CoinPayments.net to an external wallet and then into the exchange Luno. A subpoena is required to obtain further information beyond the Luno transfer. The same intelligence received for the previous address also revealed that from the payments made into CoinPayments.net, the change was paid into a BTC address also linked to CoinPayments.net. Note that the change refers to the Unspent Transaction Outputs (UTXOs). UTXOs are split into the payment to a receiver, and the change is then returned to the sender (ankura, 2024). The remaining BTC was then sent to external wallet addresses, of which some still hold BTC. One of these wallet addresses is the address bc1q##…ks3y (see Figure 5, top left inside the rectangle). From this wallet, traces of payments into the exchanges Coinbase, Binance, HitBTC and ByBit were found (refer to Figure 5). Through law enforcement, a section 205 subpoena is required to obtain account information and outgoing transactions at these exchanges.

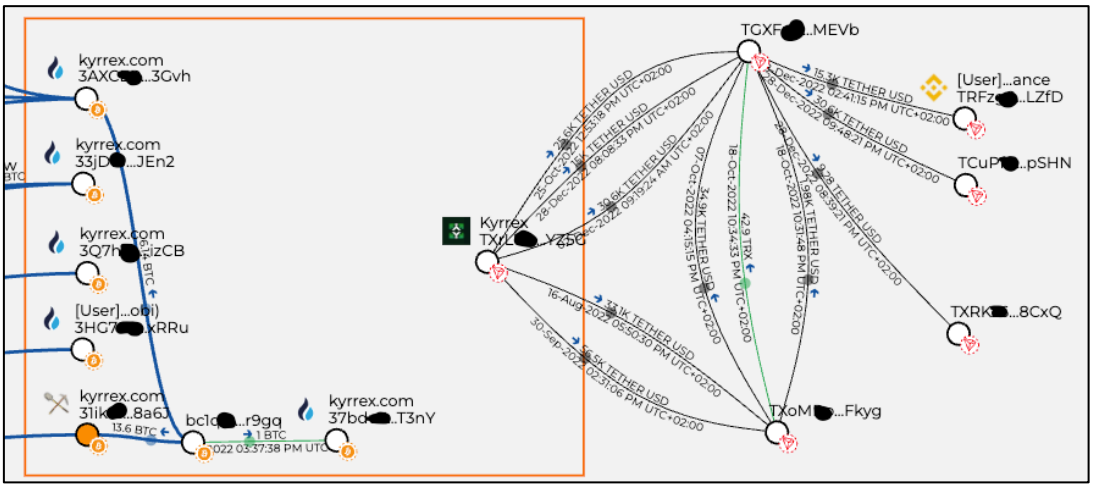

Figure 4: Outgoing Transactions From kyrrex.com

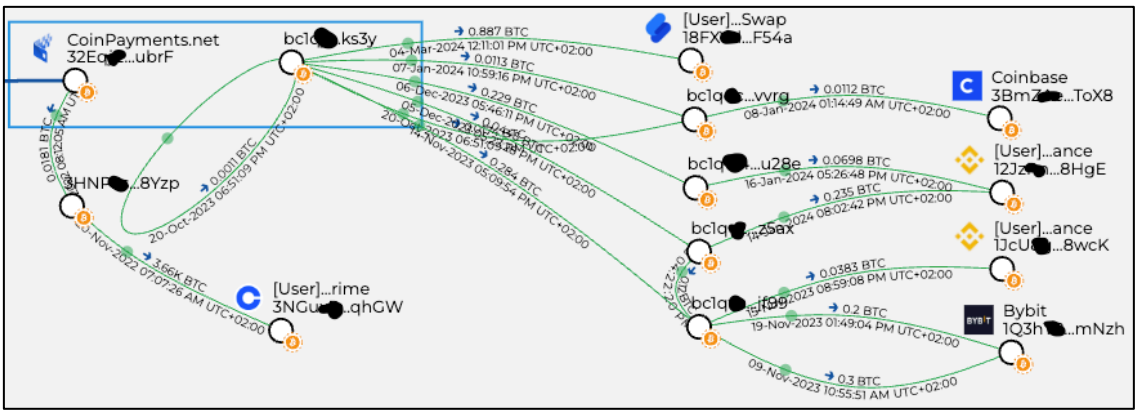

Figure 5: Outgoing Transactions from CoinPayments.net

3.3 Off-Chain Analysis

The off-chain analysis is also included in the analysis phase and overlaps with both the data collection phase and the theory development and validation phases. As the investigation moves forward, additional data and information are uncovered and gathered, while new theories are being developed and validated, refer to Figure 1.

3.3.1 Parallel path

The objective of this path is to search for a connection between each crypto address and an online presence of the address, whether it be on social media, web pages or the like.

Google searches were done on the three scammer addresses but returned no results. The AI Chat Bot for Google, Gemini (Google Gemini AI Chat Bot, 2025), was also used to see if any results could be retrieved. It returned a result that the addresses were flagged on chainabuse.com as involved in fraudulent activities. However, this was linked to the report that was filed by the analyst. Therefore, no positive results were found. This method is also categorised as Open-source Intelligence (OSINT), which is covered in the following section.

3.3.2 OSINT

OSINT involves gathering, processing, and correlating information that is publicly accessible from open data sources like social media, forums, blogs, public government data, publications, or commercial data. OSINT methodologies begin with initial input data and employ advanced collection and analysis techniques to progressively enhance understanding about a target individual or organisation. As each new piece of information is discovered, analysts move closer to their ultimate objective (Pastor-Galindo, Nespoli, Gómez Mármol, & Martínez Pérez, 2020).

In this segment of the analysis, OSINT methods are used to attempt to reveal the suspect's identity, based on the details provided by the victim as described in Section 3.1. During this phase, data collection continues as

new information is discovered online. The gathered data and information are transformed into actionable intelligence, leading to the suspect's profiling. Finally, the actionable intelligence should be converted into evidence that is admissible in court.

- Passive OSINT

Passive OSINT is the process of gathering information from publicly available sources such as Google, Whois records, Netcraft, books, articles, and similar open data repositories (Kolenbrander, 2025). In the case of an investigation, passive OSINT analysis aims to collect personal data about a target without any direct interaction with them. This method utilises various tools to find specific details, aimed at constructing a profile of the targetß individual (Botha, Singh, & Leenen, 2025a).

List of Names and Phone Numbers

The victim provided a list that included names and phone numbers from SA) and the UK. Through Truecaller (Truecaller, 2025), it was discovered that the SA numbers are linked to the ###-platform ZA Office and that these numbers are Voice-over-IP (VoIP). An additional check was conducted on claritycheck.com (a paid service for finding information on phone numbers and email addresses) (ClarityCheck, 2025), yielding no meaningful results. Searches on Google were carried out for names associated with ###-platform, and each name was connected to negative reviews on hellopeter.com and Trustpilot. The names are not allowed to be revealed in this paper. What can be disclosed is that the names are typical white male English speaking South African names, and can also be typical UK names.

Domain Name

The domain's expiration has resulted in a lack of available information online using ViewDNS.Info (ViewDNS.info, 2025). While the Wayback Machine (Wayback Machine, 2025) offered some insights, the domain's active period was brief. The domain lookup tool, who.is, provided no details, only confirming the domain's non-existence. None of the domain tools uncovered any useful data. According to the Gemini AI tool, the domain has minimal online presence, raising concerns due to the lack of basic information. Gemini suggested that the platform might be fraudulent with the intent to steal money, and it strongly recommended avoiding any interaction with it (Gemini, 2025).

On scam detector (scam-detector.com, 2025), a website that provides original information, reporting, reviews and analysis on websites, domains and e-commerce platforms, and advising if these are legitimately, safe and trustworthy, the ###-platform.io web domain got a score of 40.7% which signals risky and red flags. The domain was created on 23 June 2022, and the victim was scam started in December 2022. Shortly after the domain was created. Scam detector also indicated it has a proximity to suspicious websites of 73% and a phishing score of 78%. The website's meta data was poorly configured which would not help its online presence and loses credibility. The domain was active for 1 year, 11 months before it became inactive. Running the web domain through scam adviser (SCAMADVISER, 2025) it gave a very low trust score of 17%.

The domain www.###-platform.io was associated with negative feedback on hellopeter.com (hellopeter.com, 2025) and trustpilot.com (Trustpilot, 2023). Notably, the names and numbers given by the victim also appeared in complaints from other victims on these platforms, suggesting that the scammers targeted multiple individuals using the same identifiers. Some complaints noted that the scammers previously operated under different domain names, rs-fx.com and eduprocentre.com, indicating a prolonged period of fraudulent activity which continues with the current domain.

Another search result from Google pointed to the website www.55brokers.com, which suggests that the company ###-platform appears to operate as a UK-based entity, with the authority to provide services in the UK. Nonetheless, its regulation is solely in St. Vincent and the Grenadines, classifying it as offshore. Therefore, this is typically indicative of a scam (55BROKERS, 2025).

Email Address

The provided email address, s######s@cryptodotcom.info was subjected to various verification tools, revealing that the email account does not exist.

Regarding the names list email addresses all belonging to the domain ###-platform.io, various user complaints were found on websites like ScamAdviser, Trustpilot and Reddit, involving unsolicited emails promoting 'guaranteed' investment opportunities or recovery services for lost funds. It has been reported as 'pig butchering' or advance-fee scams, where scammers build trust via email or chat, then request deposits or

personal information. Pig butchering is an investment scam where fraudsters gain the trust of victims of time and then deceive them into investing in fake investment platforms (often fake cryptocurrency investment platforms) (DFPI, 2025).

No credible business or professional profile for any of the names were found to be linked to these email accounts in legitimate directories like LinkedIn or corporate registries.

- Active OSINT

Active OSINT typically involves the use of a program or script to collect data and leaves a log behind (Kolenbrander, 2025). Active OSINT analysis also entails interacting with a target person under deceptive circumstances, such as using a fake or undercover profile, to persuade them into disclosing personal information. This approach, however, carries a higher likelihood of the target discovering the subterfuge, potentially resulting in them changing their behaviour. It is important to emphasize that, without explicit authorization from a law enforcement body, conducting active OSINT is illegal in most jurisdictions. If such permission is granted, the information collected through active OSINT can later be used in a passive manner by scanning online platforms to gather fragmented information about the target (Botha, Singh, & Leenen, 2025a). For this investigation, no active OSINT methods were utilised. It could be considered in the near future with the legal permissions granted.

3.4 Link Analysis

Link analysis is the identification of relationships and connections between two entities such as individuals, organisations, etc (Holzer, Dietz, & Yang, 2016). 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. By employing OSINT techniques on the data provided by the victim, a number amount of relevant information was successfully gathered. However, not enough data could be retrieved to successfully identify a target suspect. When collecting information on a target, a case management strategy is needed to keep track and make sense of the findings. For this case, the link analysis and case management tool used was Maltego (see Figure 6). Link analysis remains a component of the analysis stage, as well as of the theory formulation and verification stage. However, the main focus is placed on the suspect identification and reasonable grounds phase, refer to Figure 1.

Referring to Figure 6, the top left section illustrates the victim connected to her mobile number, email address, and a link to ABSA bank. Funds were moved from ABSA bank to the cryptocurrency exchange VALR. The BTC address associated with VALR is the victim's BTC deposit address at VALR. The three BTC addresses connected to the victim's address are those of the scammers, to which funds were transferred from the victim’s address and account at VALR. This data was acquired through a subpoena by law enforcement. The remainder of the blockchain link analysis is not included in this graph, as it was already illustrated in detail using the Breadcrumbs tool, as shown in figures 2, 3, 4 and 5. The three scammer addresses are connected to the entity ###-Platform. All information available on the platform is linked to this entity, including the domain name, email addresses, lists of phone numbers from the UK and SA, and a list of names (likely pseudonyms) of individuals who contacted the victim. WhatsApp chat messages between the victim and suspects have been retrieved and stored in Maltego. However, these chats did not yield further insights into the scammers’ personal details beyond the fake names used. Connections were made to the websites hellopeter.com and trustpilot.com. Numerous negative reviews were found and associated with the platform name, and the names from the list provided by the victim also appeared in these negative reviews.

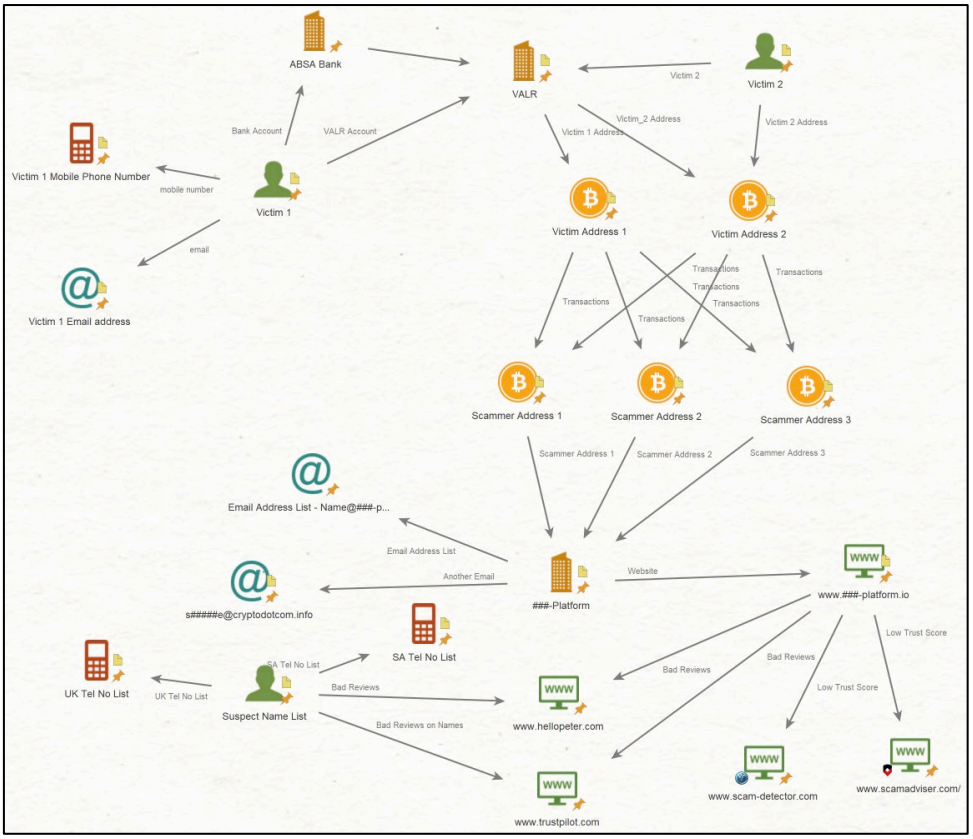

Figure 6: Link Analysis

3.5 Law Enforcement Function

This segment of the investigation is part of the legal action phase, refer to Figure 1, and is conducted by legal authorities to locate and prosecute the suspect, initiating the process of charging, arresting, imposing sanctions, recovering assets, and seizing funds.

In this study, certain legal actions were performed. The cryptocurrency exchange VALR received a subpoena and was instructed to disclose the personal information of the account holder along with all outgoing transactions. This information was obtained and proved to be highly beneficial for this investigation. Additionally, a subpoena was sent to the exchange kyrrex.com to provide the personal details of the account holder and outgoing transactions, but no information has been received yet. Nevertheless, through a law enforcement contact, intelligence was able to acquire the outgoing transactions. The account holder's user name was also obtained; however, it was not useful as the registered name was 'M Mpayme', which is a made-up name.

Unfortunately, the identities of the scammers remain undisclosed, and this phase cannot be fully executed without sufficient intelligence and evidence to proceed. Scammers are sufficiently adept at hiding their traces. The best hope is to follow the funds on the blockchain, conducting on-chain analysis, with the hope that the scammers make a mistake and leaks certain information that could be used in the off-chain analysis. A follow up study will be done in the near future that will focus mainly on the off-chain analysis. Ultimately the goal is to obtain the identity of the scammers and bring them to justice.

4. Process Evaluation

By employing a case study approach, the process can be tested and refined in practical scenarios. Previous studies conducted by the authors focused on a number of cases that has also follow the proposed process and with each case the process was progressively refined. The initial development of the process can be found in the analysis of the MTI Crypto Investment Scam" (Botha, Pederson, & Leenen, 2023). Another example involved an investigation into the fraudulent use of BTC in a divorce proceeding (Botha & Leenen, 2024). The same principles were applied in this case, particularly in relation to tracing funds on the blockchain. Following the second case, the process was further refined in another study, which introduced a high-level methodology describing how OSINT is applied in blockchain investigations (Gertenbach, Botha, & Leenen, 2024). A third incident involving a

cryptocurrency giveaway scam was investigated and followed the proposed process. This process was then refined once more in a subsequent study. (Botha, Singh, & Leenen, 2025a). Another case on a crypto fake investment scam was done following the refined process (Botha, Singh, & Leenen, 2025b). The specific case examined in this paper followed the refined process with the aim of determining where it could be further improved.

The investigation process offers a structured and systematic method for tackling cryptocurrency crime investigations. It underscores the necessity of collecting data from diverse sources to construct a comprehensive view of illegal activities. A significant emphasis is placed on clustering and pattern analysis, fundamental techniques in blockchain analytics, crucial for revealing the identities behind cryptocurrency transactions. The process also highlights the importance of link analysis and visualisation, which are critical for understanding complex transaction networks and for communicating findings to stakeholders.

The process is crafted to be practical and relevant for real-world investigations by law enforcement, financial institutions, and other organisations. OSINT techniques are crucial in this approach for associating blockchain activities with a particular individual or entity. The off-chain section of the process does not provide enough detail. Enhancements could include offering specific guidance and additional details on the techniques employed at each stage. While the on-chain analysis is detailed, the off-chain analysis and OSINT sections could benefit from more depth and examples. Examples of suspicious transaction patterns should be highlighted, and metrics on how the process was evaluated should be included. As blockchain technology and related investigative methods are continually advancing, the proposed process should be regularly updated to incorporate these developments.

5. Conclusion

With the growing adoption of blockchain technology, there's a corresponding increase in crimes and scams related to cryptocurrency. This paper offers practical insights by evaluating a structured investigative process that was previously proposed by the authors, relevant to law enforcement, regulators, investigators, analysts and researchers. The evaluation is done by taking a case study and follow the steps and phases proposed by the previously proposed methodology. This particular case study involves an elderly woman who was deceived by a fraudulent investment scheme. The case is currently under investigation by the CSIR (Council for Scientific and Industrial Research) in collaboration with South African law enforcement. No personal details of the victim have been disclosed in this paper. All cryptocurrency addresses and transactions have been masked to prevent complete identification of the addresses and transactions. The perpetrators persuaded the victim to transfer money using BTC, facilitated through the BTC blockchain. The proposed methodology or process is divided into five distinct phases, each accompanied by several steps. These steps often span multiple phases, meaning some steps might be part of two or three phases simultaneously. The steps include initiating a criminal case, conducting on-chain and off-chain analysis, and running a concurrent process for each cryptocurrency address to search for matches across social media platforms, forums, blogs, dark web markets, and more. OSINT techniques are employed, and link analysis is performed to visualise all collected data, making it understandable for external parties like law enforcement agencies. The information collected is transformed into actionable intelligence, which is then turned into evidence that is admissible in court. The final step involves legal procedures to prosecute and apprehend the suspect or target. The document offers a comprehensive assessment of the proposed procedure by analysing a specific case, highlighting its strengths and suggesting areas for improvement. Online scams continue to pose a major global threat due to the absence of standardised and official laws. Additionally, the borderless nature of cryptocurrency transactions has led to a rise in these scams within financial and cyber-crimes. In addition to evaluating the proposed process for investigating cryptocurrency crimes, this paper also aims to increase awareness about fake investment scams and fraudulent cryptocurrency investment platforms.

Ethics Declaration: Ethical clearance was not needed for this research.

AI Declaration: The academic AI tool Writefull was used to improve my English in the paper. The Gemini AI chat bot was used to see if I could find additional information on the scammer names, phone numbers and email addresses.

References

55BROKERS. (2025, Oct 20). *Is RSI-FX a scam or legit?* Retrieved from www.55brokers.com: https://55brokers.com/trader-inquiry/mr-51

ankura. (2024, Apr 25). *Crypto Asset Investigations: Key Considerations and Pitfalls*. Retrieved from ankura: https://angle.ankura.com/post/102j5sp/crypto-asset-investigations-key-considerations-and-pitfalls

AnyDesk. (2025, Oct 31). *Home Page*. Retrieved from anydesk.com: https://anydesk.com/en

Botha, J., Pederson, T., & Leenen, L. (2023). An Analysis of the MTI Crypto Investment Scam: User Case. *European Conference on Cyber Warfare and Security* (pp. 89-99). Athens, Greece: Academic Conferences International Limited.

Botha, J., & Leenen, L. (2024). Cryptocurrency-crime investigation: Fraudulent use of bitcoin in a divorce case. *International Conference on Cyber Warfare and Security (ICCWS)* (pp. 34-42). Johannesburg: Academic Conferences International Limited.

Botha, J., Singh, K., & Leenen, L. (2025b). Analysis of a Cryptocurrency Investment Scam: Pig Butchering. *European Conference on CyberWarfare and Security (ECCWS)* (pp. 61-70). Kaiserslautern: Academic Conferences International Limited.

Botha, J., Singh, K., & Leenen, L. (2025a, 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/

Chainalysis.com. (2020, Oct 9). *Why You Can't Trace Funds Through Services Using Blockchain Analysis (And Why You Don't Need to Anyway).* Retrieved from Chainalysis.com: https://www.chainalysis.com/blog/blockchain-analysis-trace-through-service-exchange

ClarityCheck. (2025, Oct 18). *Reverse Phone Lookup*. Retrieved from claritycheck.com: https://claritycheck.com

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

DFPI. (2025, Oct 31). *Pig butchering – how to spot and report the scam*. Retrieved from Department of Financial Protection & Innovation (DFPI): https://dfpi.ca.gov/news/insights/pig-butchering-how-to-spot-and-report-the-scam/

Gemini. (2025, Oct 28). Gemini Chat Bot. *Information on rsi-platform.io*.

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

Google Gemini AI Chat Bot. (2025, Oct 26). *https://chaton.ai/gemini/*. Retrieved from https://chaton.ai/gemini/: https://chaton.ai/gemini/

hellopeter.com. (2025, Oct 12). Retrieved from hellopeter.com: https://www.hellopeter.com/rsi-platform-daniel-miller

Holzer, C., Dietz, J., & Yang, B. (2016). Employing Link Analysis for the Improvement of Threat Intelligence Regarding Advanced Persistent Threats. *5th IAJC/ISAM International Conference* (p. 11). Orlando, Florida: International Association of Journals & Conferences (IAJC).

HTX. (2025, Oct 23). *Home Page*. Retrieved from HTX: https://www.htx.com/

Kolenbrander, J. (2025). Privacy Research using Active OSINT Techniques (p32). Virgina: Ph.D. thesis, Virgina Tech.

Pastor-Galindo, J., Nespoli, P., Gómez Mármol, F., & Martínez Pérez, G. (2020). The Not Yet Exploited Goldmine of OSINT: Opportunities, Open Challenges and Future Trends. *IEEE Access, 8*, 10282-10304.

SCAMADVISER. (2025, Oct 26). *SCAMADVISER*. Retrieved from https://www.scamadviser.com/check-website/rsi-platform.io

scam-detector.com. (2025, Oct 10). *Scam Detector Validator*. Retrieved from scam-detector.com: https://www.scam-detector.com/validator/rsi-platform-io-review

The Banking Association Aouth Africa. (2024, Dec 11). *Press Briefing Notes-Enhancing-DPCI-Capabilities.* Retrieved Oct 31, 2025, from banking.org.za: https://www.banking.org.za/wp-content/uploads/2024/12/press-briefing-notes-enhancing-dcpis-capabilities.pdf

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/

Trustpilot. (2023, Oct 18). *RSI-Platform.io Review*. Retrieved from Trustpilot: https://www.trustpilot.com/review/rsi-platform.io

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

Wayback Machine. (2025, Oct 25). Retrieved from Wayback Machine Internet Archive: https://web.archive.org/

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