A Proposed High-Level Methodology on How OSINT is applied in Blockchain Investigations

Wian Gertenbach[1], Johnny Botha[2], Louise Leenen[3]
[1,2]Council for Scientific and Industrial Research, Pretoria, South Africa
[3]University of Western Cape and CAIR, Cape town, South Africa
[1]wgertenbach@csir.co.za
[2]jbotha1@csir.co.za
[3]lleenen@uwc.ac.za

Abstract:
The characteristics of blockchain established a desirable platform for entities to innovate and operate in a secure, transparent, and decentralised manner. However, cybercriminals have increasingly found refuge in the decentralised environment of blockchain technology. Cryptocurrencies are increasingly misused in malicious activities that encompass the trade of illicit goods, money laundering, various types of scams and ransomware attacks. The total cryptocurrency value received by illicit addresses reached an all-time high of $20.6 billion in 2022 according to Chainalysis. The inherent privacy and anonymity features of many blockchain networks make it challenging for law enforcement and regulatory agencies to track and apprehend wrongdoers. Consequently, a pressing need arises not only to initiate investigations on the blockchain to identify unlawful activities, but also to discover connections between these activities and the identities of the responsible individuals. Due to blockchain data being publicly available, the application of Open-Source Intelligence (OSINT) techniques is proposed to facilitate these types of investigations. In the context of blockchain, OSINT, together with investigation tools hold the promise of unearthing valuable information that could aid in attributing malicious activities to the individuals responsible for those actions. By analysing and synthesizing data from publicly accessible sources, such as data from blockchain explorers and link analysis tools such Chainalysis, Maltego or Spiderfoot, investigators could potentially unveil valuable clues that assist in building a comprehensive picture of blockchain-related criminal activities. Ultimately, with sufficient information and actionable intelligence collected, the main goal is to link it to Know Your Customer (KYC) data, that could be obtained from cryptocurrency exchanges via a subpoena from law enforcement agencies. This paper delves into the mechanisms of various OSINT tools and techniques, to determine their adaptability to the specific demands of blockchain investigations. This study provides a methodology and recommendations with insights into how these tools can be wielded to bridge the gap between blockchain's pseudonymity and real-world identities.

Keywords: Blockchain, OSINT, Cryptocurrency, Blockchain-investigation, Cybercrime

1. Introduction and Background

Blockchain technology, a distributed digital ledger, is the core of almost all cryptocurrencies. The technology laid the foundation for Bitcoin and was introduced by Satoshi Nakamoto in his white paper *"Bitcoin: A Peer-to-Peer Electronic Cash System[1]"* (Di Pierro, 2017). An increase in the number of copies of a database distributed across a network result in a corresponding factor increase in the decentralisation of the ledger and the complexity of hacking the system. Blockchain can store various types of data, typically including cryptocurrency transactions, Non-fungible Token (NFT) ownership and Decentralised-Finance (DeFi) smart contracts. Blockchains are unique due to their decentralised nature and the fact that they are immutable ledgers (Rodeck & Curry, 2022).

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 for intelligence purposes (Steel, 2007). In cybersecurity, OSINT can be used in ethical hacking to discover digital footprints and to identify threats and vulnerabilities. Breached data plays a significant role for attackers to collect relevant information to prepare for an attack. However, breached data can also be very handy for investigators to gather intelligence on target individuals (ioSENTRIX, 2023).

The adoption of blockchain technology has increased in recent years. However, due to some of the characteristics of cryptocurrency, so has crime in this space, attracting many scammers and fraudsters. Cryptocurrency eliminates the need for a middleman; direct transactions occur between two individuals (Botha, Botha, & Leenen, 2023). Cryptocurrency allows the execution of transactions pseudo-anonymously, where funds

[1] https://bitcoin.org/bitcoin.pdf

can be moved across national borders with limited oversight by governments. Transactions are recorded, publicly available and visible to anyone. However, no personal information is visible on the blockchain. Investigators need to follow the funds on the blockchain up to a point where the target individual attempts to “cash-out” via an off-ramp. An example of such an off-ramp is a cryptocurrency exchange. In this research study, an address linked to an off-ramp is referred to as a destination address, see Figure 1. Exchanges should maintain KYC data that investigators can request via a subpoena with the assistance of law enforcement (Botha, Pederson, & Leenen, 2023; Alden, Brown, & Tucker, 2021).

This paper focusses on some of the major challenges that online investigators face with blockchain crimes. OSINT plays a big role in online crime investigations. However, the tools and techniques to assist in blockchain crime investigations are still a grey area. This paper explores several tools relevant to blockchain investigations and aims to illustrate how OSINT techniques can be adapted to the specific demands of blockchain-related investigations. The paper contributes towards the body of knowledge by proposing methodology and recommendations on how OSINT can be applied in blockchain investigations.

2. Blockchain Investigation Challenges

Investigating malicious activities on the blockchain has become a critical, but challenging endeavour. Cryptocurrencies have increasingly been used by criminals for easy money laundering, illicit goods trading, – terrorist financing campaigns and scams (Reddy & Minnar, 2018). There are several key reasons, described in sections below, why cybercriminals have adopted the blockchain as their playground for illicit transactions.

2.1 Pseudo-Anonymity

The pseudo-anonymous nature of the blockchain allows criminals to remain relatively hidden, as transaction records only store wallet addresses rather than actual names. This poses a significant challenge in cryptocurrency crime investigations. Transaction history is publicly available on the blockchain, but a user only needs the wallet address of the receiver to send a payment, keeping the receiver’s identity unknown (Kuzuno & Karam, 2017). This makes it challenging for investigators to trace and identify the individuals involved in scams and illicit activities. Unlike banking infrastructure, where both parties depend on a bank to process transactions, blockchain transactions occur in a decentralised environment. Globally, many banks have implemented account monitoring systems to safeguard against financial fraud (Ting-Hsuan, 2020). Furthermore, banks also enforce KYC regulations, which aim to verify a customer’s identity and to identify potential risk factors related to fraud and other financial crimes (Lowe, 2022). This is advantageous from an investigative standpoint because banks can maintain records of transactions between users, making it easier to detect and investigate fraudulent activities.

2.2 Tracking of Funds

It is difficult to directly trace the flow of funds on the blockchain because criminals often use tumblers and mixers to hide the true destination of the funds. Cryptocurrency mixing or tumbling is a technique of obscuring the origins of a crypto transaction through mixing one’s tokens with others of the same type through thousands of transactions and multiple paths (Botha, Pederson, & Leenen, 2023). Investigators may observe that a target individual has transferred cryptocurrencies to a mixer, and another party has received it. However, discerning a direct connection between the parties remains elusive. This method is widely used by criminals, and it capitalises on the opacity of transactions, hindering straightforward tracing of funds and complicating investigative efforts (Stylianou, 2022).

2.3 Unregulated Environment

The cryptocurrency sector is mostly unregulated compared to traditional fiat currencies. Criminals often make use of unregulated exchanges that do not enforce KYC or AML (Anti Money Laundering) requirements. Frequently located in high-risk countries with low KYC/AML standards, these exchanges often have no obligation to provide information when foreign authorities issue a subpoena as part of a money laundering investigation (Stylianou, 2022).

3. The Role of Open-Source Intelligence

OSINT is crucial for intelligence gathering and investigations as it offers valuable insights for decision making and strategy. Blockchain transactions and cryptocurrency activities are publicly available information and transparent to a certain degree. Investigators will perform on-chain analysis, on the blockchain. When on-chain analysis has reached a pivotal point, where a specific address can be identified as an end or destination address, off-chain OSINT comes in to play to provide a more comprehensive understanding of a suspect, target individual or entity. OSINT and off-chain analysis allow the identification of connections between individuals and the uncovering of relevant information or intelligence that is not available from on-chain data alone (CryptoInvestigators, 2023).

3.1 OSINT Tools and Techniques

This section explores various tools widely used in the industry for performing on-chain and off-chain analysis and intelligence gathering. An investigator would also require a case management tool for linking data, information, actionable intelligence and evidence. Popular case management tools are IBM i2 Analyst's Notebook, Maltego and Spiderfoot.

3.1.1 On-Chain

When a cryptocurrency scam or crime investigation is initiated, an investigator will receive cryptocurrency addresses as inputs, without any personal information about the target or suspect. Blockchain explorers, such as Blockchain.com, are the most important tools for investigations on cryptocurrency crimes. They can assist in tracing transactions, analysing patterns and understanding user activities. Each block provides data about the blockchain, cryptocurrencies, tokens, smart contracts, transactions, wallet addresses, timestamps and more (OSINT Team, 2017). However, it is very difficult to follow the flow of funds and transactions when using these blockchain explorers on their own. Various tools have been developed to improve visualisation and link analysis that are of great value to investigators (Table 1). Tool prices are included for reference. Most of the tools require a yearly subscription fee (per annum(p.a.)) for the full version.

Table 1. On-Chain Tools

Tool	Description	Price
Chainalysis Reactor	The ideal solution to investigate, analyse and link cryptocurrency transactions on the blockchain to real entities. The tool also allows for the monitoring of suspicious addresses and makes searches based on identifiers. Automatic searches through social media and Dark web sites are performed and allows to visualise which entity manages a specific wallet address (Chainalysis, 2023).	Options between $67 000 – 100 000 p.a.
Maltego	A powerful tool to perform link analysis and investigations. The tool can be used together with various other tools integrated into the solution, both free and proprietary. This allows an investigator to obtain additional data to build a case and link on-chain data to off-chain data and real-world entities. The additional integrated tools are called transforms which could add functionality from people searches, email searches, cell-phone number searches, social media searches, Dark web searches, Search Engine searches, etc. For Maltego to be able to perform any intelligence gathering, on-chain or off-chain, the tool needs to connect to external data-sources via a transform. Cipertrace (ciphertrace, 2023) and Tatum (Tatum-Team, 2022) are the two known transforms for crypto investigations (Mikhnovich, 2021).	+-$2000 p.a. (excluding paid transforms. A transform such as cypertrace is +-$2000 p.a. on top of the price of Maltego)
QLUE	A tool designed by law enforcement for investigators in the financial crime investigations to secure evidence of fraud that involves cryptocurrency. The tool is capable of linking and visualising thousands of transactions and wallet addresses, and it also has a clustering capability. It will, for example, cluster all addresses that are linked to exchanges together or several addresses that are potentially linked to the same individual. It also has monitoring capabilities and will send	Received a quote for $2000 p.a.

	alerts when funds are being moved from suspected addresses (QLUE, 2023).	
Ciphertrace	This tool continuously monitors crypto transactions for compliance violations and trigger events. The tool has capabilities for anti-money laundering (AML), sanctions and travel rule compliance. In addition, it measures crypto exposures from destination and origin of fiat funds and it can perform risk analysis and fraud detection. The tool has financial investigation capabilities and can collaboratively explore suspicious crypto activity, uncover money laundering, trace stolen funds and illicit payments (ciphertrace, 2023).	+-$2000 p.a.
Breadcrumbs	A more affordable solution that has monitoring and blockchain investigation capabilities. With its pathfinder capability is can find the shortest route of the flow of funds from origin to destination addresses. In addition, it has OSINT tools that can explore the Dark web. The tool caters for several blockchains such as Bitcoin, Ethereum, Polygon, Solana, Tron, and any ERC-20 Token *(tokens created on the Ethereum blockchain)* (breadcrumbs, 2023).	Various options, depending on the number of searches required. The basic option is $100 p.a., the individual-pro $500 p.a., and the team-pro $2000 p.a.

The investigator will follow the funds by using one of the tools in Table 1 up to a point where possible personal information can be obtained, for example from an exchange via a subpoena.

3.1.2 Off-Chain

Once some personal information has been obtained, the investigation shifts to an off-chain path, meaning away from the blockchain. The type of information could include an email address, cell-phone number, name and surname, social media account handles, and more. Two types of OSINT approaches are considered when selecting the appropriate software: passive and active. The passive approach is the most commonly used method, where an investigator will collect publicly available information on the Internet. An active approach is a more targeted method for obtaining data when the required information is hidden. For example, an investigator might use a shadow profile to connect with target individuals on Facebook to learn more about them. Specific software is not necessary for active tactics, as many tools can assist in this strategy. Several tools are available for conducting investigations using passive OSINT techniques. Some of the most used tools are listed below (not in any order of preference).

Table 2. Off-Chain Tools (SEON, 2023)

Tool	Description	Price
Maltego	The tool has access to various databases and has great visualisation and link analysis tools. One major let-down of the tool is that its user interface is outdated compared similar tools. Also see the description in Table 1. This tool can be used for both on-chain and off-chain analysis.	+-$2000 p.a.
Google Dorks	A method to perform advanced searches on search engines.	Free
SEON	Great gathering of social media information with scalable API calls.	Starts at $599
Lampyre	Very good for due diligence, cyber treat intelligence and crime analysis.	$300 p.a.
Recon-ng	Open-source scripts in Kali Linux for gathering technical information about website domains.	Free
Spiderfoot	Specifically designed for investigations with over 200 modules for data collection and analysis. The tool was acquired by Intel471 in Nov 2022.	Pricing information has been removed after the Intel471 takeover.

IBM i2 Analyst's Notebook	Allows to quickly collate both structured and unstructured data into powerful visualisations that assists in identifying actionable intelligence. The tool can integrate with various data sources and has social network analysis capabilities (IBM Security, 2023).	Base version starts at $7160 p.a. with the premium version at $19200 p.a.
Start.me Dashboards	Online OSINT resources are multiple and various and new tools arises every other day. Start.me allows to create dashboards and allows to categorise tools for various OSINT categories such as tools for email, Name searches, cell-phone searches, etc. In addition, the tool allows for linking multiple dashboards built by other investigators (Start.me, 2020).	Free. The pro version is $24 p.a. or $70 one-time fee
OSINT Frameworks	Various online tools and frameworks (OSINT Framework, 2023)	Free
CSI Linux	A Linux distribution that is a complete cyber forensics platform. Most of the tools mentioned above is already installed in this distribution (Welcome to CSI Linux, 2023).	Free. Some of the installed tools requires licensing.

Note that the list of tools mentioned in Tables 1 and 2 are only a number of the popular tools used in industry today. Many more tools are available than those listed here. With so many tools and options available, it is difficult to know when to use which tools and for which purpose. Section 4 proposes methodology on how OSINT tools can be applied to assist in blockchain investigations.

4. Proposal for Applying OSINT in Blockchain Investigations

An investigative methodology has been developed as a proposed solution to adapt specific OSINT tools in the blockchain investigation process. Figure 1 depicts a flow diagram outlining the steps and tools for investigators to follow when investigating a blockchain-related crime. The diagram has been partially derived from the methodology highlighted by Nick Furneaux in his book *Investigating Cryptocurrencies: Understanding, Extracting, and Analysing Blockchain Evidence* (Furneaux, 2018). The book describes a methodology for investigating blockchain that includes detecting the use of cryptocurrencies in a crime, analysing an address, following the money, and monitoring addresses. This paper integrates Furneaux's methodology with the investigative process utilized by *TCG Forensics*, a company based in South Africa. Botha et al.'s paper, *An Analysis of the MTI Crypto Investment Scam: Use Case*, validates the success of this methodology, marking and confirming several addresses as destination addresses for which a subpoena could be issued at the linked exchanges (Botha, Pederson, & Leenen, 2023). The proposed methodology in this paper expands on Furneaux's and TCG Forensics' processes by including the use of OSINT during specific stages of the investigation. The methodology is in the pipeline to be tested by the designated point of contact within the South African Police Service (SAPS).

In this paper it is assumed that the investigation starts with a cryptocurrency address and that the investigators do not know whether the address is linked to a hot/online or a cold/hardware wallet, exchange decentralised exchange (DEX) or any other platform on the blockchain where the address can be linked to. A hot wallet is a cryptocurrency wallet software application that is connected to the Internet through a computer or phone, whereas a cold wallet is a hardware device that is offline (Ramirez, 2023).

To initiate a case, investigators will receive a cryptocurrency address by the victim reporting the crime. This address may belong to either the victim or the suspect. In cases where only the victim's address is provided, the suspect's address can be identified by tracing the funds from the victim's address back to the point at which they were deposited into the perpetrator's account. The investigation then proceeds along two parallel routes. One route involves on-chain analysis, while the other entails an attempt to establish a link between the address and public data sources. Multiple addresses may surface as a possible destination address during the on-chain investigation. For each trace to a new address identified as a potential destination while following the funds, investigators will attempt to find information on social media or other public sources. If a link is found, the investigator can use OSINT to search social media sites, forums and websites to gather additional information about the target. Any information associated with the address will most probably be fake and won't point to the real person (Lomas, 2023). If no link to public data can be established, investigators will stop the OSINT approach for that specific address and continue with the on-chain analysis. It is important to note that the on-chain analysis never stops unless a destination address has been identified and KYC can be obtained. As the case advances, investigators will build a comprehensive suspect profile, incorporating all the relevant information collected from both on-chain and off-chain analysis and OSINT investigations. This entire procedure is streamlined through the utilisation of case management software, an essential tool for efficient organisation and coordination as mentioned in section 3.1.

On-chain analysis involves analysing all possible information to be found on the blockchain for the target address, including extracting valuable data, following funds and monitoring activity. A wealth of information can be accessed by visiting a blockchain explorer for the specific currency associated with the given address. The investigators can then start following the funds and analyse the data of the transactions which will provide valuable insight into where funds came from and where they went on the blockchain. Breadcrumbs, QLUE, Ciphertrace, Tatum, Maltego (via Transforms for Ciphertrace and Tatum) and Chainalysis Reactor are suitable for this application as it can assist blockchain investigations by automating link analysis and fund following. This is an important step to find a possible destination address from where the funds have potentially been moved to an exchange. The data can be analysed in two ways: through a literal interpretation and an analysis of the implicit information that the data can suggest. An example of what data can infer is filtering transaction data based on date and time, which allows for the identification of trade patterns and providing an opportunity for temporal analysis. Addresses and transactions can also be flagged as suspicious, providing the investigator with more insights in future investigations.

Investigators will follow the flow of funds on the blockchain repeatedly. Ultimately, the whole process loops until the investigators can establish if the funds have been moved to a legitimate cryptocurrency exchange or any other form of off-ramp. If the connection or link can be made to an exchange, the investigators can issue a subpoena with the help of law enforcement to obtain KYC data and bank details about the target. With the KYC data the investigators can move to an off-chain analysis and request to freeze the address and account on the exchange so the funds cannot move any further.

In the event where the funds have not been moved to an exchange, the target most likely keeps the funds in a cryptocurrency wallet where they remain stationary for an extended period or held within an unregulated and/or DEX. Investigators can deploy a sensor via tools such as QLUE, Cyphertrace or Breadcrumbs to trigger a notification when the funds are moving again. From there the funds will be followed again with the hope that it is moved via to an exchange or any form of off-ramp.

If KYC data could be obtained, the investigation will shift to an off-chain analysis. This phase involves processing and gathering information about the target, conducting OSINT and link analysis to help build a suspect profile. Identity documents, a proof of address and an email address are key examples of KYC data. These pieces of information will empower investigators with information that serves as an input for the off-chain OSINT investigation. Establishing this baseline proves crucial as the investigation advances, providing a foundation for gathering more intricate details about the target. It is important to note that the information needed varies significantly depending on the unique characteristics of the case under investigation.

A few tools and techniques can be applied for the specific information required, see Table 2. OSINT Frameworks is a good starting point as it lists tools in an expandable mind map form, with a long list of use cases to choose from. The investigator can isolate the required tools and establish an OSINT tool dashboard on Start.me for easy accessibility. Advanced searches can be performed with Google Dorks to find specific information that is not readily available through normal search queries. Recon-ng is a useful tool for conducting web-based reconnaissance and gathering preliminary information about the target and can be used by investigators to collect information about domains, IP addresses, email addresses, and various online entities.

In the case where a social media handle or profile name linked to the target address is identified, investigators can initiate the process by leveraging Social Media Intelligence (SOCMINT). This involves gathering profile details, community interaction information and post metadata. Criminals will often post addresses on social media sites when executing impersonation or giveaway scams. SEON, Maltego with OSINT transforms and Spiderfoot, connected to various data sources via APIs, are appropriate tools to use to identify these fraudulent activities and analyse data. Active OSINT can also be employed to engage with the target using a shadow or undercover profile, facilitating the acquisition of more extensive information. However, with active OSINT there is higher risk of being discovered by the target, potentially leading to altered behaviours. The data gathered from active OSINT can then be used passively by enumerating online platforms and extracting bits and pieces of information about the target. Link analysis can be performed using tools such as Analyst’s Notebook, Maltego, Lampyre and Spiderfoot to evaluate relationships between the information gathered from different sources.

Most of the OSINT (off-chain) tools mentioned in this paper come pre-installed on the CSI Linux distribution. It is a Linux distribution containing the necessary tools to conduct OSINT investigations. It is specifically designed to be used as a complete investigation and digital forensics platform. It also contains custom case management software that can be used to build a suspect profile. It should be noted that one must still pay license fees for the paid software tools on the distribution.

As the investigation progresses, the suspect profile will continuously be updated. Once the comprehensive suspect profile has been developed, and information gathered through both on-chain analysis and off-chain (OSINT) investigation has reached a point where it can be transformed into actionable intelligence, the case is ready for transition to law enforcement for further in-depth scrutiny and potential prosecution. This transition marks the critical point at which the meticulously collected data and insights can be converted into evidence, become instrumental in initiating legal actions against the identified individual or entities involved in cryptocurrency-related illicit activities.

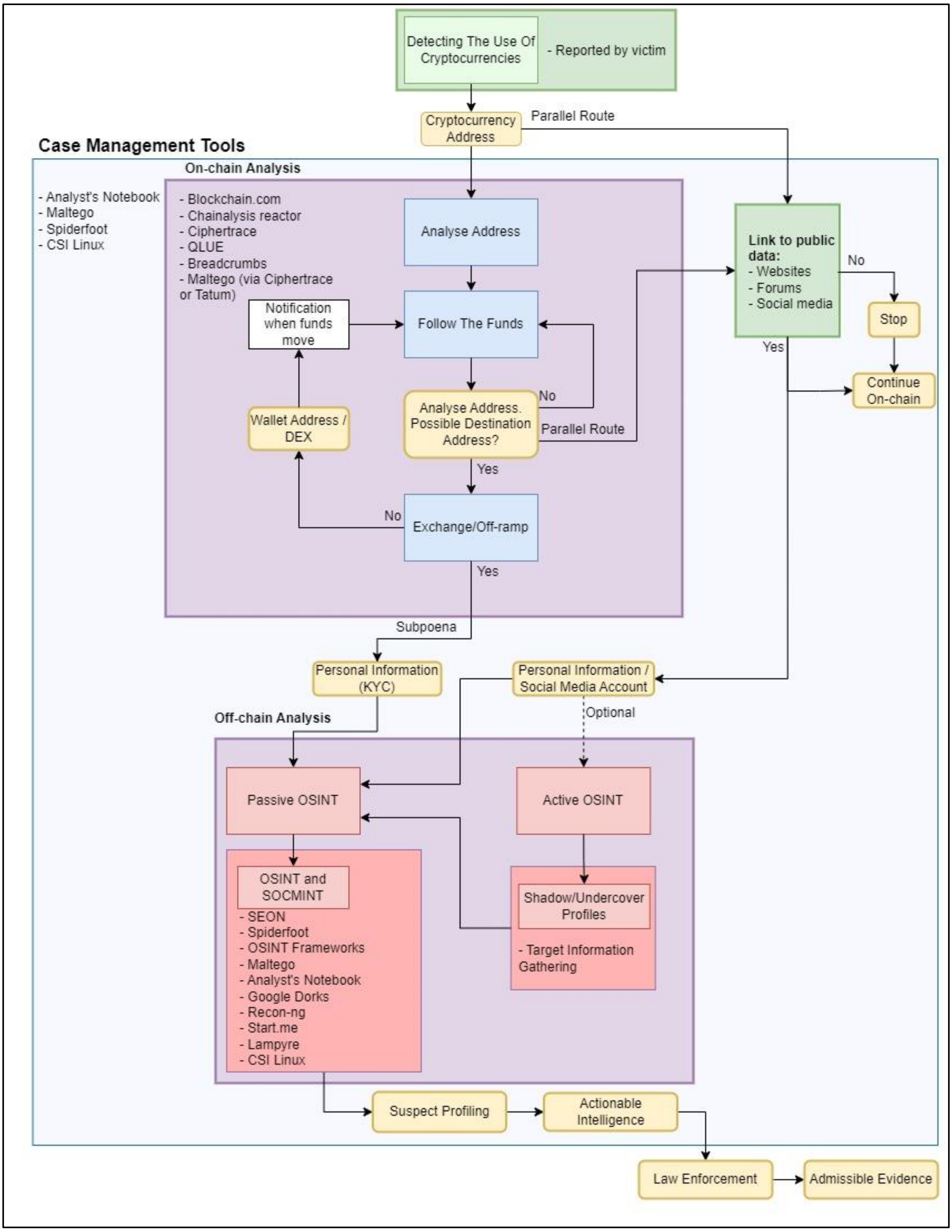

Figure 1: Investigation methodology incorporating specific OSINT tools.

5. Recommendations

The recommended methodology is to follow the steps outlined in Figure 1. Case management software is expensive, and the choice of the best tool will depend on the investigator’s budget. Analyst’s Notebook is the most expensive, followed by Maltego and Spiderfoot.

On-chain analysis is still a new area of specialisation, and most of the tools in this field are still extremely expensive. Refer to Table 1 for the prices of the on-chain analysis tools. Chainalysis is the most expensive, followed by QLUE, Ciphertrace and Maltego. Maltego can integrate via two transforms, namely Cipertrace and Tatum. Tatum is a free transform and would be the preferred option. The Cipertrace transform provides additional functionality but at an extra cost. Breadcrumbs is a more affordable option that has been launched recently. However, with the more affordable package, the number of searches may be limited. For research and small cases, this would be the preferred option due to affordability. In terms of recommending the best solution, Chainalysis and QLUE provides the most features and functionality and are the most suitable options for those with a substantial budget. Ciphertrace and Maltego are well-suited for a moderate budget but with some limitations. Breadcrumbs is considered the optimal choice for those seeking a free and more affordable option, depending on the number of searches required prices vary.

For off-chain analysis and OSINT tools, one would mostly want to opt for the free and cheaper tool options. See Table 2 for the costing of tools. Google Dorks is free with tons of information gathering capabilities. Recon-ng is a good solution for technical data gathering on websites and web domains. The OSINT framework and Start.me dashboards are free to use and introduces a vast number of tools to assist in various types of investigations. However, several of the tools listed in these frameworks are not free. Quality data comes at a cost. Investigators would want to keep to free information gathering tools up to a point where it might be necessary to make use of a few paid solutions. Spiderfoot is a highly recommended link analysis tool and comes with a free and paid version. The tool links to a number of free as well as paid data sources via API calls. SEON is a great tool for gathering social media information with scalable API calls and fairly affordable.

A well recommended option is CSI Linux. This choice would require a degree of Linux and tech savvy to make use of this distribution but would ultimately be of great assistance in any cybercrime investigation. The browser on the distribution has several dashboards, frameworks and plugins pre-installed. It comes with Maltego installed, as well as various other OSINT and information gathering tools.

6. Conclusion

The pseudo-anonymous, unregulated, and rapid expansion of the blockchain provides criminals with a means to misuse cryptocurrencies for activities like money laundering, scamming and illicit trading. This poses a challenge for investigators and law enforcement agencies, as they must adapt to the ever-evolving landscape of digital currencies and blockchain technology to effectively combat these illicit activities. The importance of OSINT is emphasized as a valuable tool for intelligence gathering and decision-making because blockchain transactions and cryptocurrency activities are publicly available and somewhat transparent. The paper suggests that investigators should conduct on-chain analysis within the blockchain to identify specific addresses and follow transactions. Once this on-chain analysis reaches a point where KYC data can be obtained, off-chain OSINT becomes crucial in providing a more comprehensive understanding of a suspect involved in cryptocurrency-related activities.

An investigative methodology is proposed, which integrates a set of tools and steps to assist in cybercrime investigations. Investigators need to construct a comprehensive suspect profile by integrating all pertinent information gathered from both on-chain and off-chain analysis and investigations. To facilitate this process, the paper underscores the importance of utilizing case management software as an essential tool for efficient organization and coordination. Specific tools like Maltego, Analyst's Notebook and Spiderfoot that can aid in this regard are mentioned. For the on-chain analysis, tools such as Breadcrumbs, Maltego (via Ciphertrace and Tatum transforms), Chainalysis Reactor, Ciphertrace (standalone tool) and QLUE can assist by automating the process of following funds and performing link analysis. Off-chain analysis can be assisted by OSINT tools such as SEON, Start.me, Analyst’s Notebook, Recon-ng, Lampyre, OSINT Frameworks, Maltego, Spiderfoot, Google Dorks, and various others. Each case will have different requirements for the type of information to be collected, and any corresponding tool can be used to satisfy these unique requirements. Once the suspect profile reaches a stage where the gathered intelligence can be transformed into admissible evidence, the case is transferred to law enforcement for further examination.

This paper indicates that there is no single definitive tool to use when investigating cryptocurrency crimes. A list of tools that may greatly assist in such an investigation is mentioned. Moreover, a methodology is proposed, which integrates OSINT and investigative tools to assist with blockchain investigations. Tools are recommended based on the quality of data it can obtain and its corresponding price. Free tools should be used to gather information up to a point where more intricate data is required. Ultimately, a combination of tools and techniques will be required to conduct a successful investigation and is heavily dependent on the type of crime committed and the information gathered.

7. References

Alden, P., Brown, C., & Tucker, R. (2021). Using Blockchain Analysis From Investigation to Trial. *DOJ Journal of Federal Law and Practise*, 59.

Botha, J., Botha, D., & Leenen, L. (2023). An Analysis of Crypto Scams during the Covid-19 Pandemic: 2020-2022. *18th International Conference on Cyber Warfare and Security, ICCWS 23* (pp. 36-48). Towson University, Baltimore County: Academic Conferences International Limited.

Botha, J., Pederson, T., & Leenen, L. (2023). An Analysis of the MTI Crypto Investment Scam: User Case. *22nd European Conference on Cyber Warfare and Security, ECCWS 2023* (pp. 89-99). Hellenic Air Force Academy andthe University of Piraeus, Athens, Greece: Academic Conferences International Limited.

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

Chainalysis. (2023, Oct 11). *Chainalysis Reactor*. Retrieved from https://www.dataexpert.eu/: https://www.dataexpert.eu/products/security-solutions-producten-chainalysis/chainalysis-reactor/

ciphertrace. (2023, Oct 11). *Cryptocurrency intelligence*. Retrieved from https://ciphertrace.com/: https://ciphertrace.com/

CryptoInvestigators. (2023, Oct 11). *OSINT Investigations, OSINT Gathering & Analysis*. Retrieved from https://cryptoinvestigators.com/: https://cryptoinvestigators.com/osint/#:~:text=OSINT%20is%20a%20crucial%20tool,activities%20of%20individuals%20and%20entities.

Di Pierro, M. (2017). What is Blockchain. *Computing Prescriptions*.

Dyson, S., Buchanan, W. J., & Bell, L. (2018, November 20). The Challenges of Investigating Cryptocurrencies. *The Journal of The British Blockchain Association, 1*(2). doi:https://doi.org/10.31585/jbba-1-2-(8)2018

Furneaux, N. (2018). *Investigating Cryptocurrencies: Understanding, Extracting, and Analyzing Blockchain Evidence.* Indianapolis, Indiana, US: John Wiley & Sons, Inc.

IBM Security. (2023, Oct 13). *IBM i2 Analyst's Notebook*. Retrieved from https://www.ibm.com/: Automatic OSINT Analysis for i2 Analyst's Notebook

ioSENTRIX. (2023, Oct 11). *How OSINT is used in cybersecurity*. Retrieved from https://iosentrix.com/: https://iosentrix.com/blog/How-OSINT-is-used-in-Cybersecurity-Part-1/

Kuzuno, H., & Karam, C. (2017). Blockchain explorer: An analytical process and investigation environment for bitcoin. *2017 APWG Symposium on Electronic Crime Research (eCrime)* (pp. 9-16). Scottsdale, AZ, USA: IEEE. doi:10.1109/ECRIME.2017.7945049

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

Lowe, J. (2022, November 2). *What is KYC? Financial regulations to reduce fraud*. Retrieved October 11, 2023, from Plaid: https://plaid.com/resources/banking/what-is-kyc/

Mikhnovich, V. (2021, Dec 9). *Cryptocurrency Investigations with Maltego: Tips & Tricks for Bitcoin and Ethereum*. Retrieved from https://www.maltego.com/: https://www.maltego.com/blog/cryptocurrency-investigations-with-maltego/

OSINT Framework. (2023, Oct 13). *OSINT Framework*. Retrieved from https://osintframework.com/

OSINT Team. (2017, Sep 1). *Cryptocurrency OSINT Investigations: A detailed guide to Block Explorers*. Retrieved from https://osintteam.blog/: https://osintteam.blog/cryptocurrency-osint-investigations-a-detailed-guide-to-block-explorers-69cf25daf5da

QLUE. (2023, Aug 11). *QLUE Home Page*. Retrieved from www.qlue.io: https://qlue.io

Ramirez, D. (2023, Jul 11). *Crypto Hot Wallet vs. Cold Wallet: What's the Difference*. Retrieved from nerdwallet: https://www.nerdwallet.com/article/investing/hot-wallet-vs-cold-wallet

Reddy, E., & Minnar, A. (2018, September 1). Cryptocurrency : a tool and target for cybercrime. *Acta Criminologica : African Journal of Criminology, 31*(3), 71-92. doi:10.10520/EJC-14d902942d

Rodeck, D., & Curry, B. (2022, Apr 28). What is Blockchain? (pp. 92-95). IEEE. Retrieved from https://communications.pasenategop.com/: https://communications.pasenategop.com/wp-content/uploads/sites/15/2022/06/What-Is-Blockchain.pdf

SEON. (2023, Oct 12). *List of 10 Best OSINT Tools*. Retrieved from https://seon.io/: https://seon.io/resources/comparisons/osint-software-tools/

Start.me. (2020, Nov 23). *How to Manage your OSINT resources best with start.me [Expert opinion]*. Retrieved from https://blog.start.me/: https://blog.start.me/osint-resources-experts/

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

Stylianou, A. (2022, April 4). *Cryptocurrencies - The challenges for criminals and investigators*. Retrieved October 13, 2023, from Global Compliance Institute: https://www.gci-ccm.org/insight/2022/01/cryptocurrencies-challenges-criminals-and-investigators

Tatum-Team. (2022, Jan 4). *Using Maltego and Tatum to Track the Money Trail of a Bitcoin Scam*. Retrieved from https://tatum.io/blog: https://tatum.io/blog/using-maltego-and-tatum-to-track-the-money-trail-of-a-bitcoin-scam

Ting-Hsuan, C. (2020). Do you know your customer? Bank risk assessment based on machine learning. *Applied Soft Computing, 86*.

Tuwiner, J. (2023, October 29). *How Long Do Bitcoin Transactions Take?* (C. Aulds, Editor) Retrieved December 4, 2023, from buybitcoinworldwide: https://buybitcoinworldwide.com/tx-time/

Welcome to CSI Linux. (2023, Oct 13). Retrieved from https://csilinux.com/