IJECBE

IJECBE (2025), **3**, **2**, 411–432
Received (21 May 2025) / Revised (25 June 2025)
Accepted (28 June 2025) / Published (30 June 2025)
https://doi.org/10.62146/ijecbe.v3i2.135
https://ijecbe.ui.ac.id
ISSN 3026-5258

International Journal of Electrical, Computer and Biomedical Engineering

RESEARCH ARTICLE

Illicit Cryptocurrency Investigation Digital Forensic Framework: Integrating Off-chain and On-Chain Analysis for Two Types of Crime

Oliva Regina[†], Kalamullah Ramli[*†], and Abdul Hanief Amarullah[‡]

[†]Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia, Depok, Indonesia
[‡]National Cyber and Crypto Agency of Indonesia
[*]Corresponding author. Email: kalamullah.ramli@ui.ac.id

Abstract

Cryptocurrencies have become integral to contemporary financial infrastructures; however, their pseudonymous architecture presents substantial challenges for digital forensic investigations. This study introduces the Illicit Cryptocurrency Investigation Digital Forensic Framework, a novel model that systematically integrates both on-chain and off-chain investigative techniques into a unified forensic process. In contrast to previous studies that isolate blockchain analysis from traditional digital forensics, the proposed framework merges blockchain transparency with contextual digital evidence to enhance investigatory coherence. Validated through expert judgment by digital forensic practitioners, the framework is tailored to address two principal categories of cryptocurrency-related crimes: Type A, where the investigation originates from suspect-controlled devices, and Type B, where blockchain transactions serve as the initial investigative lead. By structuring the process from identification through reporting, the framework promotes evidentiary integrity, procedural traceability, and legal admissibility across diverse jurisdictions. This research contributes a practical foundation for addressing the increasing complexity of illicit cryptocurrency investigations.

Keywords: Digital Forensics, Cryptocurrency Crime, On-Chain, Off-Chain, Cybercrime, Blockchain Investigation

1. Introduction

Cryptocurrency usage has seen a remarkable surge in recent years, driven by its innovative technology and numerous advantages, including cross-border transactions, lower costs, and enhanced financial inclusion for unbanked populations [1]. However,

this rapid adoption has coincided with a significant increase in cryptocurrency-related crimes. The Chainalysis 2025 Crypto Crime Report highlights a considerable rise in illicit activities such as money laundering, ransomware attacks, and the purchasing of illegal goods on dark web marketplaces[2]. Cryptocurrencies' pseudo-anonymous nature often complicates transaction tracking, leading to severe challenges for law enforcement agencies attempting to curb these illicit activities.

The growing role of cryptocurrency in various forms of crime highlights how its transparency creates unique opportunities for investigation. According to the 2024 Chainalysis report, illicit trade volumes are expected to reach record levels as on-chain crime becomes more diverse and professionalized. While illicit on-chain activities were previously mostly associated with cybercrime, cryptocurrencies are now also being used to fund and facilitate a wide range of threats, from national security to consumer protection. As digital currencies gain broader acceptance, illicit on-chain activities have become increasingly varied. For instance, some criminals primarily operate off-chain but move funds on-chain for the purpose of money laundering [2].

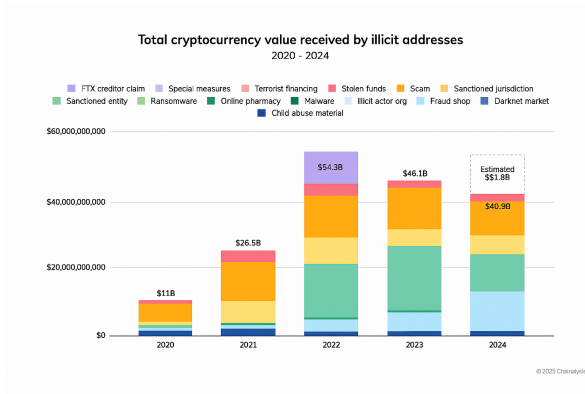

Figure 1. Total Cryptocurrency value received by illicit address [2]

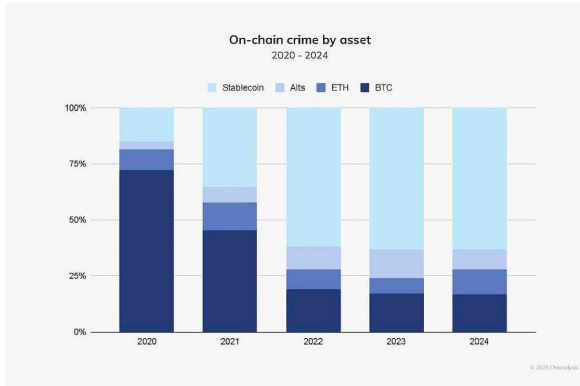

Figure 2. On-chain crime by asset [2]

In Blockchain Technology, based on the transaction process, data obtained from the blockchain can be classified into on-chain and off-chain data [3]. Each of these methods plays a crucial role in understanding how digital currency transactions function and their broader implications on the financial system [4]. On-chain analysis involves examining data directly stored on the blockchain. Every cryptocurrency transaction, whether Bitcoin, Ethereum, or others, is recorded in the public ledger, ensuring transparency and creating an immutable record of all transactions [5]. In contrast, off-chain analysis focuses on data outside the blockchain, such as transaction details from exchanges, social media sentiment, and user behavior. This approach takes into account external factors that can influence cryptocurrency prices, such as news or market sentiment collected from social media platforms.

Digital forensics is becoming increasingly crucial in the world of cryptocurrency due to the rising number of crimes involving digital currencies, as mentioned in the previous paragraph. Criminals often exploit the anonymity provided by digital currencies to engage in illegal activities such as money laundering, ransomware attacks, and fraud [2]. As noted by Raza et al., digital forensic investigations are essential for tracking funds and gathering evidence, which are key to prosecuting these crimes. The ability to recover and analyze digital evidence from cryptocurrency wallets can lead to significant advancements in criminal investigations, enabling law enforcement to combat financial crimes more effectively [6].

Research on the various dimensions of crimes related to cryptocurrency continues to evolve. We identified studies that focus on cryptocurrency forensic investigations. Most of the research concentrates on on-chain analysis [7], [8], [9], [10], [11] which examines transaction records on the blockchain, or off-chain approaches [7], [12] ,[13], [14], [15], [16]which analyze data outside the blockchain, such as user behavior and transaction patterns across different exchanges. However, none of these studies have yet proposed a cryptocurrency forensic model or how to present digital evidence in cases of cryptocurrency misuse for criminal activities. Meanwhile, according to the Chainalysis report, cryptocurrency crimes continue to grow, causing both material and financial losses.

Research on the various dimensions of crimes related to cryptocurrency continues to evolve. Existing studies primarily focus on either on-chain analysis—which examines transactional records encoded on blockchain networks—or off-chain approaches, which analyze user behavior, device logs, and exchange-level interactions. While both streams contribute valuable insights, they tend to operate in silos, and none have proposed an integrated forensic model that systematically connects these two domains. More critically, limited attention has been given to how digital evidence should be structured and preserved when cryptocurrency is misused as part of criminal operations. As highlighted in recent reports, the magnitude and complexity of crypto- enabled crimes are rapidly increasing, leading to substantial financial losses and widening the gap between law enforcement capabilities and technological realities.

In response to these multifaceted challenges, this paper introduces the Illicit Cryptocurrency Investigation Digital Forensic Framework—a comprehensive and legally conscious forensic model specifically tailored to the dual complexities of on-chain and off-chain investigative environments.

Unlike prior studies that treat blockchain analytics and traditional digital forensics as isolated processes, this framework offers a fully integrated approach that aligns with international standards such as NIST SP 800-86[17], ISO/IEC 27037[18], and ISO/IEC 27042[19]. It has been methodically validated through expert judgement involving practitioners from digital forensics and cybersecurity fields, ensuring both technical robustness and field-level applicability.

The framework is operationalized through two primary crime typologies: Type A, which begins with identified suspects and relies on off-chain digital evidence such as seized devices and user logs; and Type B, which initiates from anonymized on-chain activities such as suspicious wallet transactions or smart contract traces. This dual-path structure accommodates investigative flexibility while maintaining evidentiary integrity, chain-of-custody, and cross- jurisdictional admissibility. The novelty of this study lies in its systematic unification of on- chain and off-chain forensic dimensions within a legally sound, practitioner-ready model—one that bridges investigative theory and real-world criminal justice needs in the rapidly evolving landscape of crypto-enabled crime.

This paper is structured into six major sections. Section 2 outlines the theoretical and procedural foundations of digital forensics and blockchain analysis, including a synthesis of relevant literature. Section 3 classifies the typologies of cryptocurrency-related crimes that frame the investigative challenges. Section 4 presents the proposed framework, detailing its processes and legal grounding. Section 5 provides a comprehensive discussion on its adaptability, operational relevance, deanonymization strategies, legal admissibility, and expert validation. Finally, Section 6 concludes the study by summarizing its contributions and identifying avenues for further research and refinement.

2. Literature Review

The primary aim of this section is to define the phases and processes of digital forensics, including blockchain analysis, which encompasses both on-chain and off-chain elements. Additionally, it summarizes a selected framework that focuses on cryptocurrency forensics.

2.1 Digital Forensic Investigation

A Digital Forensic Investigation (DFI) refers to the structured and scientific process of identifying, acquiring, analyzing, and presenting digital data in a manner that is legally admissible and forensically sound. This process is not merely technical, but is grounded in recognized standards and legal considerations that ensure evidentiary reliability across various jurisdictions [20]. According to the widely cited NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response [17], digital forensic investigations typically follow four core phases: collection, examination, analysis, and reporting. Each phase serves a critical function in maintaining the integrity, traceability, and reproducibility of digital evidence. Complementing NIST's model, the ISO/IEC 27037:2012 standard provides detailed guidelines for the identification, collection, acquisition, and preservation of digital evidence[18].

It emphasizes the importance of procedural transparency, the role of trained personnel, and the use of forensically sound tools. Meanwhile, ISO/IEC 27042:2015 focuses on the analysis and interpretation of digital evidence, providing methodological clarity to ensure that forensic conclusions are based on verifiable and reproducible findings[19]. In the context of blockchain investigations, these standards are increasingly relevant due to the distributed and immutable nature of the underlying data structures. Prior studies, such as Mas'ud et al. [7] conducted a survey of 11 academic works in blockchain forensics and synthesized their investigative stages. The majority of these studies emphasize transaction-level analysis and evidence handling but vary in the degree to which they align with established forensic guidelines. To provide a clearer understanding of how blockchain-specific investigations map onto broader forensic principles, Table 1 presents a synthesis of digital forensic phases in the context of blockchain, as interpreted from the surveyed literature.

Table 1. Digital Forensic Processes In Blockchain

Phases	Description of Phases
Identification	The process of detecting, recognizing, and determining the nature of an incident or crime is essential for initiating an investigation. Identifying an incident or crime leads to the formulation of a hypothesis regarding the events that may have occurred. An investigation may then focus on gathering evidence to support or refute a case, or on validating the authenticity of the information at hand. During the identification phase, the questions outlined in the 5WH model should always be addressed. These questions aid in developing a hypothesis based on the information that triggers the investigation
Collection and Preservation	The collection phase involves the process of acquiring or copying data from digital devices, using forensically sound methods and techniques to create an exact digital replica. Metadata related to a case should be linked to the potential evidence, whether it is a physical device or a data file. This metadata may include information such as the case name, case number, the examiner (digital forensics investigator or investigators), timestamps, the case and seizure locations, and time zone. Evidence integrity refers to maintaining the evidence in its original form without any alterations, whether intentional or accidental. To ensure this integrity is preserved, the concept of digital fingerprinting is employed. This process uses cryptographic (or one-way) hash functions, where the input is a bit stream from a file, disk, or partition, and the output is a unique hash or signature for that input stream. By comparing the hash of the original evidence to that of its copy, one can confirm that the copy is identical to the original
Examination and Analysis	The preparation and extraction of potential digital evidence from collected data sources is a critical step in the investigation process. In digital forensics, triage refers to the process of quickly identifying the most relevant data. This is particularly important when time and resources are limited, as it allows investigators to prioritize key evidence. The goal is to process information that directly supports the investigation's objectives, determining the facts surrounding an event, assessing the significance of the evidence, and identifying the responsible parties. Once the data is prepared, it is analyzed using various methods such as statistical techniques, manual analysis, understanding protocols and data formats, linking multiple data objects (e.g., via data mining), and constructing timelines. Additionally, maintaining the chain of custody is essential to ensure the preservation and traceability of the collected data throughout the analysis phase.
Reporting	The examiner communicates the findings from the analysis phase through reports to the relevant parties. The final report should encompass all pertinent case management details, outlining the context and background of the investigation, the investigators involved, and the aspects that were examined. The documentation created during the digital forensics investigation, along with recommendations and expert testimony, will constitute the final presentation. The evidence and the methods used to obtain it are then presented either in a court of law or to a corporate audience.

2.2 Blockchain Analysis

Based on the transaction process, data obtained from the blockchain can be categorized into on-chain and off-chain data [21]. On-chain data refers to the information resulting from activities or transactions that occur directly on the blockchain and are recorded in a decentralized ledger. Off-chain data refers to information recorded outside blockchain technology, such as data noted on an exchanger.

Meanwhile, based on the analysis process, cryptocurrency transactions can be divided into two categories based on the data source. The first is on-chain analysis, which involves the examination of data recorded on the blockchain. The second is off-chain analysis, which entails the examination of data that exists outside the blockchain but is related to cryptocurrency transactions [11].

2.2.1 On-Chain

In on-chain analysis, analysts focus on finding information about the movement of funds on the blockchain. Due to the pseudonymous nature of cryptocurrency, the goal is to find cash- out points or exchangers that have implemented Know Your Customer (KYC) according to regulations. Analysts trace the Crypto Fund Flow trail by performing in on-chain analysis clustering, account ownership analysis, and e-discovery [8]. Transaction data that enters the exchanger is data collected as initial information in the off-chain analysis process. On-chain analysis analyzes data on:

- Transactions recorded on the blockchain (e.g., sender, recipient addresses, amount, and timestamp).
- Transaction patterns (e.g., frequency, amount, and relationship between addresses).
- Use of smart contracts or decentralized applications (dApps).

2.2.2 Off-Chain

In off-chain analysis, the focus is on exploring the relationship between blockchain data and real-world entities. Information derived from on-chain analysis can be utilized for Know Your Customer (KYC) processes, enabling the identification of individuals associated with specific transactions. Following the establishment of the identity behind a transaction, it is essential to conduct a digital forensic examination to gather electronic evidence from devices controlled by the suspect, which may be linked to the cryptocurrency wallet or the identified transactions. This digital forensic analysis involves scrutinizing and evaluating volatile memory, network memory, and virtual hard disks [7].
Off-chain analysis analyzes data on:

- User identities registered on centralized exchanges or crypto platforms.
- Fiat transaction records (eg, bank transfers or credit cards).
- Data from crypto wallet service providers or third parties.

2.3 Related Works

After understanding the concepts of On-Chain and Off-Chain analysis, we conducted a comprehensive review of previous research studies related to cryptocurrency forensics. This review aimed to identify and map whether these prior studies focused primarily on On-Chain analysis, Off-Chain analysis, or a combination of both. By systematically examining the methodologies used in these studies, we were able to evaluate the scope of their forensic approaches and assess the extent to which they addressed the complexities of illicit cryptocurrency transactions.

Table 2. Previous research in Digital Forensic of Blockchain

No	Name	Year	Type of Crime	Forensic Framework
1	Park et all., [12]	2023		✓
2	Holmes & Buchanan, 2023., [13]	2023		✓
3	S. Taylor et al., [14]	2022		✓
4	Salisu et al., [8]	2023		✓
5	Wu et al., [9]	2021		✓
6	Mas'ud et al [7]	2021		✓
7	Koerhuis et al., [15]	2020		✓
8	Infante et al., [16]	2024		✓
9	Meiklejon et al., [10]	2013		✓
10	Zheng et al., [11]	2021		✓
11	Chainalysis [2]	2025	✓	
12	Kethineni S, Cao Y [22]	2020	✓	
13	Alnasaa et al., [23]	2022	✓	
14	Ibrahimi A, Arifi B[24]	2022	✓	
15	Hiramoto N, Tsuchiya Y[25]	2020	✓	
16	Paquet-Clouston et al., [26]	2019	✓	

3. Type of Crime Using Cryptocurrency

According to a report by the FBI, there was a significant increase in cryptocurrency-related crimes, with a sixfold rise observed between the years 2015 and 2018 [22]. Factors that Facilitate Crime with Cryptocurrency include:

1. Anonymity, users can make transactions without revealing their identities.
2. Transaction speed, money can move between countries in seconds without intermediaries.
3. Lack of regulation, many countries do not yet have clear laws regarding the use of cryptocurrency in crime.

Cryptocurrency is frequently utilized as a method for laundering money from traditional crimes such as corruption and embezzlement. The use of crypto assets is significantly and positively associated with corruption capital and control [23]. Cryptocurrency facilitates transactions without intermediaries and without disclosing the user's identity. While cryptocurrency presents great potential in the financial realm, it also carries a high risk of corruption and financial crime due to its anonymity and lack of regulation [24]. We further categorize this misuse of cryptocurrency as a **type A crime**, where the crime has been uncovered, but law enforcement officers need to gather evidence and information regarding the movement of embezzled funds.

Additionally, cryptocurrency is frequently used in cybercrimes, including ransomware and darknet markets[2] [26] [25]. Moreover, we categorize cryptocurrency abuse as a **type B crime**. In type B crimes, the perpetrators are entirely anonymous as they operate in cyberspace, necessitating a method for de-anonymization.

4. Proposed Framework

In this study, we propose the Illicit Cryptocurrency Investigation Digital Forensic Framework—a comprehensive, structured model that seamlessly integrates both on-chain and off-chain investigative techniques. This framework is developed as a response to the increasingly sophisticated nature of cryptocurrency-enabled crimes, which often require bridging the gap between blockchain-based transactional data and conventional digital evidence.

Unlike prior approaches that tend to treat blockchain analysis and traditional digital forensics as distinct domains, the proposed framework brings them together into a unified, process-driven model. While the initial structure draws inspiration from previous research in blockchain forensics[7], the framework represents a methodological advancement by aligning explicitly with internationally recognized forensic standards, including the NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response[17], and the ISO/IEC standards 27037:2012 and 27042:2015[18][19].

These standards serve as the foundation for ensuring that every stage of the investigation—from evidence identification and collection to analysis and reporting—is not only technically sound but also legally admissible across multiple jurisdictions. By doing so, the framework addresses both the operational and judicial requirements of modern digital forensic investigations.

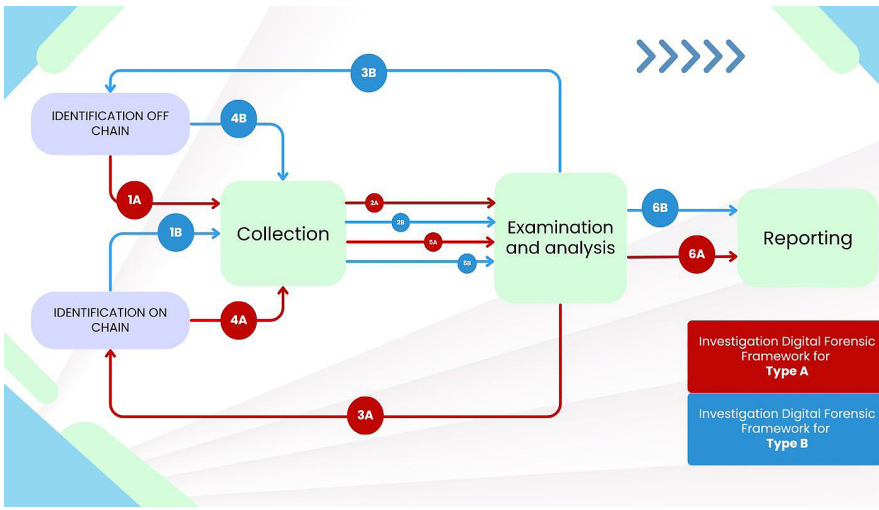

Figure 3. Proposed Illicit Cryptocurrency Investigation Digital Forensic Framework

This model is designed to support investigative workflows for two primary crime typologies, as outlined in Section 3:

1. Type A crimes, where investigators begin with tangible or digital off-chain evidence (e.g., confiscated devices, browser logs, wallet backups), and then trace transactions on the blockchain to reconstruct financial trails.

2. Type B crimes, where the investigation starts with blockchain activity linked to unidentified actors, requiring advanced deanonymization methods before real-world attribution can be established through off-chain follow-up.

The framework emphasizes interoperability and adaptability, recognizing that effective cryptocurrency investigations often involve multiple stakeholders, diverse tools, and legal systems with varying evidentiary requirements. To that end, it incorporates principles such as:

1. Forensically sound evidence acquisition, using hashing and imaging in compliance with ISO/IEC 27037.
2. Structured analytical processes, as described in ISO/IEC 27042, to support reproducibility and reliability.
3. Documentation and reporting protocols, that satisfy chain-of-custody and court presentation standards in both civil and common law systems.

To ensure empirical grounding, we conducted a systematic review of 16 peer-reviewed publications across blockchain and cyber forensics. The investigative phases—Identificati
Collection and Acquisition, Examination and Analysis, and Reporting—are mapped comprehensively to both on-chain and off-chain data sources. Each phase is further contextualized within the broader structure of the framework and aligned with best practices drawn from NIST and ISO models.

The visual structure of the framework is illustrated in Figure 1, and the methodological mapping to previous research is summarized in Table 3. Collectively, these elements present a coherent and practical model for law enforcement and forensic practitioners seeking to navigate the increasingly hybrid landscape of cryptocurrency-related investigations.

1. **Identification**
   This phase focuses on identifying and understanding incidents or crimes, which serves as the foundation for developing investigative hypotheses. By applying the 5WH model (Who, What, When, Where, Why, and How), investigators establish initial assumptions that guide their examination. The main goal is to uncover blockchain-related evidence, thoroughly exploring the digital space to reveal critical components such as wallet addresses, transaction records, and the complex network of cryptocurrency infrastructure. Each step is carefully crafted to assemble the pieces of a complex puzzle, ultimately uncovering the underlying stories behind financial transactions within the dynamic world of digital currencies[7].

   a. On-chain
      The initial phase of a blockchain forensic investigation involves identifying the pertinent data for analysis. This step requires determining the specific blockchain platforms in question (e.g., Bitcoin, Ethereum), identifying relevant addresses, transactions, and smart contracts, and understanding the nature of the suspected illegal activities. The objective is to isolate the exact blockchain

data that is relevant to the case. Previous studies have emphasized the importance of pinpointing specific addresses and transactions associated with criminal activities such as money laundering or ransomware payments.

b. Off-chain
In the papers by [7], [12], [15], [16] his phase is described as the process of identifying all potential digital evidence sources related to the case, including devices and access logs. Meanwhile, [13] and [14] build upon previous research by refining this phase, explaining that it also involves conducting forensic triage and identifying the tools required at each stage of the investigation.

2. **Collection and Acquisition**
The meticulous process of forensic digital evidence collection begins with creating imaging of data, ensuring that every bit and byte remains untouched. To uphold the sanctity of this evidence, hash functions like SHA-256 are employed, acting as digital fingerprints that guarantee the integrity of the information, confirming that no alterations have occurred during handling. Every detail is documented with precision, from the case number and timestamp to the specific location of the evidence capture, creating a comprehensive record that facilitates meticulous tracking and exploration of the case.

   a. On-chain
   During the collection phase, investigators obtain identifiable data from the blockchain. This may involve downloading the full blockchain or extracting specific blocks, transactions, or addresses of interest [7], [11]. Given the public nature of most blockchains, this data is generally accessible without the need for a warrant. However, it is crucial that the data collection process ensures the preservation of its integrity and authenticity. To achieve this, advanced tools and techniques, including blockchain explorers and forensic software, are frequently utilized.

   b. Off-chain
   This step follows the output from the identification phase and involves the collection, storage, and handling of data representing potential digital evidence. The outcome includes activities aimed at determining the collection of digital evidence. Identified evidence will be gathered and acquired. Key artifacts to be acquired, as outlined in the research papers by [7], [12], [13], [14], [15]vinclude wallet addresses, browser artifacts, seed phrases, extended private keys, wallet-based data (user profiles, contact labels), transaction records (cryptocurrency type, total amount, sender and receiver addresses, address labels, date and time, amount, fees, account balance), wallet user machine data (wallets and client logs), file locations, and other artifacts (prefetch, iconcache, thumbcache). These efforts aim to ensure the comprehensive collection of information from the end device.

3. **Examination and Analysis**
   The process involves meticulously extracting and analyzing data from various gathered sources. A range of sophisticated techniques is employed, including data mining to unearth hidden patterns, statistical analysis for insightful interpretation, and timelining to visualize trends over time. Each method adds depth to the understanding of the data, revealing the intricate stories behind the numbers.

   a. On-chain
      According to Salisu [8], cryptocurrency analysis can be done using data mining methods such as:
      - Ownership analysis integrates multiple factors and evidence to uncover the beneficiaries and identities associated with the wallet addresses being examined
      - Clustering algorithms are used to filter, match, and identify wallet addresses that belong to the same owner. These algorithms can group thousands of addresses associated with a specific wallet, which helps to minimize confusion when separating funds. This focus allows investigators to concentrate on the goal of their investigation.
      - E-discovery is a process that gathers cryptocurrency transaction data and wallet information from the internet and personal devices. This information is then compiled into a comprehensive digital map that offers investigators a complete overview of the situation. To achieve its objectives, e-discovery typically employs various tracking techniques.

      Several theories or heuristics can be used to analyze Bitcoin [10]. This heuristic is used to determine the account control of a Bitcoin address.

   b. Off-chain
      Once all artifacts are obtained through the collection and preservation process, the output from the previous steps will be used for examination and analysis. Studies such as by [7], [12], [13], [16] describe a similar analytical method, which includes examining the "client process memory." This process involves scrutinizing public and private keys, transaction data (such as addresses, labels, transaction IDs, amounts, fees, and timestamps), contacts, passphrases, backup locations, and other valuable artifacts. Additionally, it includes examining the "user device," which covers registry files, wallet.dat, log files, debug.log, peers.dat, and other significant artifacts. In [15], the examination and analysis process is further enhanced by incorporating volatile memory analysis (including string searches, grep, and keyword searches), network traffic analysis (using Wireshark), and virtual hard disk analysis (using tools like Bulk Extractor and keyword searches).

4. **Reporting**
   Crafting in-depth reports tailored for presentation to law enforcement or clients, featuring compelling data visualizations such as dynamic cash flow graphs and thorough documentation of methodologies employed throughout the analysis. These reports not only convey essential information but also draw attention through their visual appeal, making complex data more accessible and engaging for the audience.

In addition to focusing on the type of crime involving cryptocurrency, the cryptocurrency forensic model we propose also integrates both on-chain and off-chain analysis to ensure a comprehensive examination tailored to the specific type of crime. As outlined in Chapter II, we have mapped 16 research papers based on their blockchain analysis methods.

Table 3. Cryptocurrency Forensics Framework Mapping Based on Blockchain Analysis

Forensic Framework Stages	On-Chain	Off-Chain
Identification	[7]	[7], [12], [13], [14], [16]
Collection & Preservation	[7], [8], [9], [11]	[7], [12], [13], [14], [15], [16]
Examination & Analysis	[7], [8], [9], [10]	[7], [12], [13], [15], [16]
Reporting	[7], [9]	[7], [12], [13], [15], [16]

5. Discussion

5.1 Investigative Logic and Crime Typologies in Cryptocurrency Forensics

The increasing convergence between digital assets and illicit activity has transformed the landscape of forensic investigation. In response, this study introduces an integrated framework that combines on-chain and off-chain forensic techniques to address two primary categories of cryptocurrency-related crime. This section outlines the logical flow of investigation for each crime type and demonstrates how the framework adapts its methodology to suit distinct operational conditions.

a. Types of Crime A
   Type A crimes involve identifiable suspects and tangible digital evidence. These investigations typically follow a bottom-up logic—beginning with off-chain data extracted from seized devices, such as laptops, mobile phones, or server logs. Digital forensic techniques such as disk imaging, hash verification, and volatile memory preservation ensure evidentiary integrity at this stage. These off-chain artifacts often contain contextual clues, such as login credentials, browsing history, and wallet metadata, which may link a suspect to blockchain-based activity. Once such associations are established, investigators proceed to on-chain analysis to trace transaction flows, verify wallet usage, and detect interactions with KYC-regulated exchanges. This sequential process illustrates the complementary interplay between digital evidence layers in building a coherent and legally admissible investigative narrative.

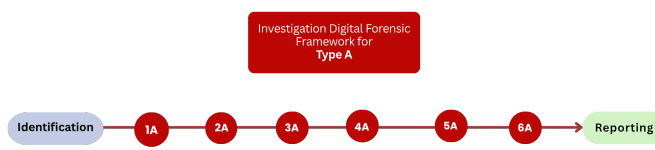

Figure 4. Illicit Cryptocurrency Investigation Digital Forensic Framework for Type A

b. Types of Crime B
Type B crimes—such as ransomware, illicit token issuance, or darknet market activity—begin with blockchain traces but lack identifiable actors. In these cases, on- chain forensic techniques are prioritized. Investigators leverage clustering heuristics, smart contract analysis, and transaction graphing to identify wallet networks and potential links to centralized platforms. Points of intersection with regulated exchanges often provide pivot points for further investigation. Off-chain attribution follows, involving subpoenas, device forensics, or OSINT-based identity tracing. This top- down approach begins with the blockchain layer and moves toward uncovering real- world identities, emphasizing the dynamic adaptability of the proposed framework.

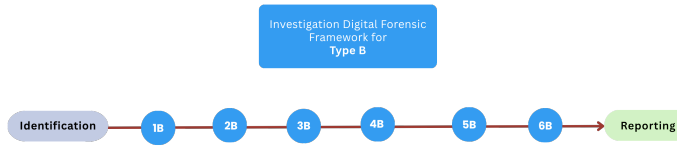

Figure 5. Illicit Cryptocurrency Investigation Digital Forensic Framework for Type B

5.2 Deanonymization Techniques in Cryptocurrency Investigations

One of the central challenges in blockchain forensics lies in the pseudonymous nature of cryptocurrency transactions. While blockchain ledgers are inherently transparent, the absence of explicit identity information associated with wallet addresses presents significant obstacles for law enforcement and forensic analysts. To address this, the proposed **Illicit Cryptocurrency Investigation Digital Forensic Framework** integrates both on-chain and off-chain deanonymization techniques to progressively reduce anonymity and support attribution in investigative contexts—particularly for **Type B cases**, where the perpetrator's identity is initially unknown.

1. On-Chain Deanonymization
On-chain deanonymization focuses on uncovering behavioral signatures and structural patterns within blockchain data. Several established techniques are employed:

   - **Multi-input Heuristics**: When a transaction includes multiple input addresses, it can be inferred that these addresses are controlled by the same entity, due to the need for all private keys to authorize the transaction [10].
   - **Change Address Identification**: By analyzing how unspent transaction outputs (UTXOs) are distributed, algorithms can often determine which output is likely the "change" address, thus narrowing down wallet ownership[27].
   - **Transaction Clustering and Graph Analysis**: Using graph-theoretic models, blockchain addresses are grouped into clusters based on recurring transaction patterns, which helps identify wallets operated by the same user[28].

- **Taint and Flow Analysis**: This technique tracks the movement of specific coins (e.g., from known illicit sources) across wallets, establishing linkages between compromised addresses and their downstream recipients [29].

2. **Off-Chain Attribution**

While on-chain methods provide structural inferences, they rarely result in conclusive identity attribution without off-chain evidence. Therefore, the framework complements on-chain analysis with external data correlation:

- **KYC-Enabled Exchange Records:** When a suspect wallet interacts with a centralized exchange that enforces Know Your Customer (KYC) protocols, investigators may obtain user identity data through lawful cooperation or mutual legal assistance treaties[30].
- **Device Forensics:** Forensically imaged devices may contain wallet software, browser artifacts, private keys, or screenshots of cryptocurrency transactions, providing direct attribution[12].
- **Open-Source Intelligence (OSINT):** Reused wallet addresses on forums, darknet marketplaces, GitHub, or social media may reveal associations between blockchain identities and online personas [31].

3. Visualizing Deanonymization Workflows
To aid practitioners in understanding how deanonymization unfolds within the framework, a simplified process illustration is provided. This visualization distinguishes on-chain techniques (highlighted in blue) from off-chain mechanisms (in red), while showing their convergence in supporting identity attribution as a figure 6.

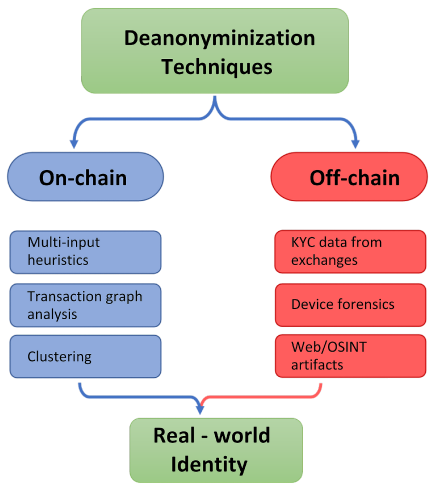

Figure 6. Deanonyminization Techniques

5.3 Expert Judgement Validation

To ensure the robustness and practical applicability of the proposed Illicit Cryptocurrency Investigation Digital Forensic Framework, a structured expert validation process was conducted. This involved three selected experts from key stakeholder institutions—namely a senior digital forensics practitioner from the Indonesian Digital Forensics Association (AFDI), a representative from the Cybercrime Directorate of the Indonesian National Police specializing in Type A illicit cryptocurrency cases, and a cybersecurity operations officer from the National Cyber and Crypto Agency (BSSN) with experience in attribution and Type B threat actor profiling. The validation aimed to assess both the theoretical soundness and operational feasibility of the framework.

Quantitative validation was conducted through a 14-item Likert-scale questionnaire categorized into four sections: (1) General Assessment of the Framework, (2) Evaluation of Each Forensic Phase, (3) Real-World Relevance and Implementation, and (4) Open-ended qualitative feedback. The Likert scale ranged from 1 (strongly disagree) to 4 (strongly agree), with a minimum standard threshold of 3.0 as the benchmark for acceptability.

Descriptive statistical analysis of the quantitative responses revealed that all items achieved an average score above the threshold. Most items scored a perfect mean of 4.00, with zero standard deviation, indicating unanimous agreement among experts. Notably, questions assessing the clarity of framework stages, integration between on-chain and off- chain procedures, and suitability for real-world investigation scenarios scored exceptionally high, reflecting both methodological coherence and applied relevance.

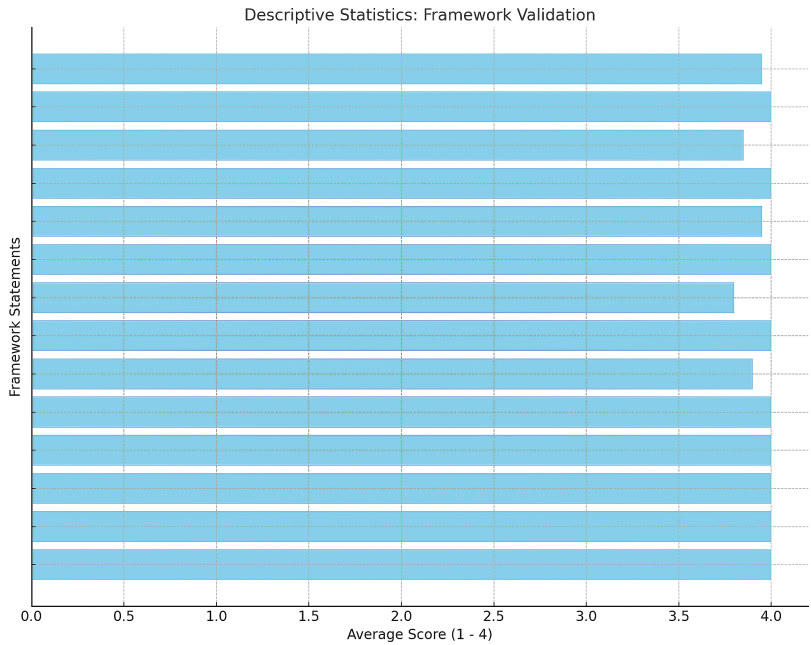

Figure 7. Descriptive Statics

A visual summary (Figure 6) highlights the average ratings per item, with a clear indication that none fell below the minimum acceptance level. This lends strong empirical support to the internal consistency and structural validity of the framework. Here is the framework statement :

PART I : General Assessment Framework

1. Does the framework have clear and easy-to-understand stages?
2. Does the framework cover all essential stages in the cryptocurrency forensic investigation process?
3. Can this framework be applied in cryptocurrency-related crime investigations?
4. Is the relationship between on-chain and off-chain analysis in this framework clear and relevant?
5. Does this framework reflect practices and standards that align with the current needs of the digital forensics industry?

PART II : Evaluation of the framework Stages

6. Is the Identification stage complete and clear for cryptocurrency investigations?
7. Does the Collection and Acquisition stage provide sufficient guidance for acquiring, recording, and preserving digital evidence from various sources?
8. Does the Examination and Analysis stage present a thorough approach to analyzing transactions and digital artifacts?
9. Does the Reporting stage provide technical and legal guidance for preparing admissible evidence reports?
10. Does each stage incorporate structured and logical integration of on-chain and off- chain analysis?

PART III : Relevance and Real World Application

11. Can this framework be practically used in real-world investigations by law enforcement agencies?
12. Does this framework provide clear procedures for selecting tools and techniques based on the needs of each case?
13. Does this framework provide effective solutions for identifying and tracing illicit cryptocurrency funds?
14. Is this framework flexible enough to be applied to various types of cryptocurrency crimes (e.g., money laundering, ransomware, illicit trade)?

In addition to the numerical assessments, qualitative feedback further enriched the evaluation. Experts emphasized that the integration of on-chain and off-chain analysis offers a comprehensive perspective for both evidentiary tracing and contextual attribution. They also noted that the phased structure—particularly the detailing of the "Collection and Acquisition" and "Examination and Analysis" stages—aligns well with practical investigative workflows, especially in cases involving pseudonymous transactions or crypto- to-fiat transitions. However, a few constructive suggestions were provided. One expert highlighted the potential to improve the documentation

standard for on-chain evidence collection to ensure admissibility in court, while another recommended expanding the framework's adaptability to encompass emerging blockchain architectures such as Layer-2 protocols or privacy coins. These insights have been acknowledged and earmarked for refinement in subsequent research iterations.

Overall, the expert validation confirms that the proposed framework is not only theoretically grounded but also operationally sound. It offers a realistic and scalable investigative model that can be adopted by law enforcement and forensic practitioners dealing with cryptocurrency-related crimes in diverse jurisdictions.

5.4 Legal Admissibility Across Jurisdictions

The legal admissibility of digital evidence—particularly in the context of cross-border cryptocurrency investigations—remains a critical yet complex issue due to inconsistencies in legal frameworks, procedural standards, and evidentiary thresholds across jurisdictions. In response, the Illicit Cryptocurrency Investigation Digital Forensic Framework incorporates established principles from internationally recognized standards to ensure that the evidence gathered is not only technically robust but also legally sustainable in diverse judicial environments.

1. Chain-of-Custody and Integrity Preservation
   To maintain the integrity and authenticity of digital evidence, the framework applies cryptographic hashing techniques—such as SHA-256—during the acquisition and preservation stages. Hash values are calculated at the point of collection and re-verified throughout the investigative process, in accordance with evidentiary integrity requirements articulated in standards such as NIST SP 800-86 [17] and the Convention on Cybercrime[32]. This approach ensures that the digital chain-of-custody remains intact, preserving the forensic soundness of the collected data.
2. Jurisdictionally Neutral Evidence Handling
   The framework adopts acquisition methods that are agnostic to specific tools or platforms, avoiding reliance on jurisdiction-bound or proprietary technologies. This ensures that exported evidence—such as blockchain transaction records, system logs, or memory captures—can be validated and analyzed using comparable forensic environments in other countries. The neutrality of the acquisition process is consistent with the guidance offered in ISO/IEC 27037:2012, which emphasizes the identification and preservation of digital evidence in a legally sound manner[18].
3. Documentation and Reporting for Legal Use
   In the reporting phase, the framework emphasizes the completeness of forensic documentation. Metadata elements—including acquisition timestamps, case identifiers, examiner credentials, hash digests, timezone indicators, and system configurations—are recorded in a structured format to support transparency and traceability. This level of documentation is essential for admissibility in courts operating under both common law and civil law traditions, as highlighted in ISO/IEC 27042:2015, which outlines best practices for forensic analysis and reporting [19].

4. Alignment with International Legal Frameworks
   The framework reflects congruence with major international instruments that govern digital evidence, including:
   - The Convention on Cybercrime[32], which provides a foundational legal framework for the collection and admissibility of electronic evidence;
   - Interpol's Guidelines on Digital Evidence, particularly relevant for blockchain-related criminal investigations[31];
   - The Financial Action Task Force (FATF) Recommendation 16[33], also known as the "Travel Rule" , which necessitates identity linkage for virtual asset transactions.

This alignment strengthens the framework's operational and legal credibility across investigative and judicial contexts.

5.5 Operational Relevance and Investigative Adaptability

The framework's strength lies not only in its structural coherence but also in its real-world applicability across diverse investigative scenarios. Its dual-modality—merging blockchain transparency with traditional digital context—creates a robust and responsive model that enhances both evidentiary rigor and operational agility. In time-sensitive cases such as ransomware attacks, the ability to swiftly identify recipient wallets, trace transactional paths, and anticipate off-ramping methods can disrupt criminal workflows and inform proactive countermeasures. Moreover, the framework emphasizes the importance of contextual interpretation; cryptocurrency-related crimes vary significantly in motive, method, and legal environment. For example, in Southeast Asia—particularly Indonesia—investigators must navigate evolving regulatory frameworks and cross-border asset tracing challenges, making adaptability essential.

A persistent challenge for the forensic community is the preservation of blockchain-based evidence. Unlike off-chain digital artifacts, which follow well-established chain-of-custody standards, on-chain data remains accessible yet volatile in terms of interpretability. There is an urgent need to standardize methods for timestamping, hashing, and documenting blockchain evidence in a legally defensible manner. Future iterations of this framework may benefit from the formalization of such protocols. Furthermore, the model invites interdisciplinary collaboration. Legal scholars, cryptography experts, behavioral analysts, and forensic practitioners must collectively interpret the distributed, pseudonymous nature of blockchain data to produce judicially admissible outcomes. As such, institutional capacity building and cross-sector training are integral to the framework's sustained relevance.

The investigative process, as reflected in this framework, is not strictly linear. Rather, it operates as an iterative loop—insights gained during one phase often necessitate revisiting previous stages. For instance, analytical findings may trigger additional data collection, while reporting outcomes may uncover new investigative leads. This adaptive design reflects the dynamic workflows typical of modern digital crime investigations.

Ultimately, the integrated framework offers a pragmatic and theoretically grounded roadmap for addressing cryptocurrency crime. It aligns technical capabilities with investigative intuition and contributes to both policy discourse and operational refinement. As digital economies evolve, this framework provides a timely foundation for strengthening the accuracy, speed, and legal robustness of digital forensic investigations involving cryptocurrency.

6. Conclusion and Future Work

This study has presented a structured and empirically grounded digital forensic framework designed to address the growing complexity of cryptocurrency-related investigations. By integrating both on-chain and off-chain forensic methodologies into a unified process model, the proposed Illicit Cryptocurrency Investigation Digital Forensic Framework effectively bridges the gap between blockchain transparency and contextual digital evidence. This integration enables a more holistic investigative approach capable of adapting to the diverse modalities and dynamic nature of crypto-enabled crimes.

The framework accounts for two principal investigative pathways: one in which digital evidence originates from seized devices and is later corroborated through blockchain analysis, and another in which the initial clues emerge from on-chain activities and are further substantiated through off-chain attribution techniques. This bidirectional adaptability allows investigators to align their forensic strategies with the available entry points and the nature of the criminal act, thereby enhancing procedural agility and evidentiary depth.

Built upon the synthesis of 16 peer-reviewed studies and validated by expert judgment from experienced digital forensic professionals, the framework demonstrates both theoretical robustness and practical relevance. Its modular structure allows for adaptation to jurisdiction- specific legal and technological contexts, ensuring broader applicability across cross-border and multi-agency investigative environments.

Looking forward, several areas require further exploration to enhance the framework's utility and responsiveness. One key direction involves the integration of automation and artificial intelligence, particularly for the detection and correlation of high-volume blockchain transactions. As cryptocurrency activity grows in scale and complexity, the application of machine learning and data mining techniques could significantly improve the speed and accuracy of forensic analysis. Additionally, the interoperability of this framework with global legal mechanisms remains a critical area for future work, especially concerning evidence exchange protocols, international compliance standards, and mutual legal assistance treaties.

Another pressing issue lies in the standardization of blockchain evidence preservation. Despite the inherent transparency and immutability of blockchain data, its legal admissibility remains challenged by a lack of consistent protocols for extraction, documentation, and presentation in court. Future research should focus on formalizing procedures for handling blockchain-specific artifacts, including smart contract interactions, transaction hashes, and metadata, to ensure that such evidence is both technically sound and legally defensible.

In conclusion, the framework proposed in this study offers a timely and structured response to the evolving challenges of cryptocurrency forensics. It provides not only a conceptual contribution to academic discourse but also a practical tool for investigators, analysts, and policymakers working at the intersection of law, technology, and finance. As digital financial ecosystems continue to evolve, this research lays a strong foundation for multidisciplinary collaboration and for the development of more resilient, adaptive, and ethically informed approaches to combating crypto-enabled crime.

Acknowledgement

The author would like to express sincere gratitude to Universitas Indonesia for providing essential academic resources and institutional support throughout the course of this research. Deep appreciation is extended to Lembaga Pengelola Dana Pendidikan (LPDP), Ministry of Finance of the Republic of Indonesia, for their financial assistance, which enabled the successful completion of this study.

Special recognition is due to Prof. Dr. Kalamullah Ramli for his invaluable academic mentorship and continuous guidance, which played a pivotal role in shaping the conceptual and methodological direction of this work. The author is also grateful to Abdul Hanief Amarullah, a practitioner from the National Cyber and Crypto Agency (BSSN), whose practical insights and technical assistance greatly enriched the research process.

This study further benefited from the expert judgement and validation provided by several professionals with domain-specific experience in digital forensics and cybersecurity. The author would like to specifically acknowledge Izazi Mubarok, Chairman of the Indonesian Digital Forensics Association; Andi Yusuf, Director of Cybersecurity Operations; and Jeffrey Bram, Investigator from the Directorate of Cybercrime. Their critical assessments, constructive feedback, and professional perspectives significantly contributed to the refinement and credibility of the proposed framework.

Lastly, the author extends appreciation to colleagues and peers who offered thoughtful comments, academic encouragement, and ongoing support throughout the writing and revision phases of this research.

References

[1] C. Chitsungo. “Harnessing Digital Strategies to Combat Cryptocurrency-Enabled Crimes: Addressing Money Laundering, Illicit Trade, and Cyber Threats”. In: *American Journal of International Relations* 9.7 (Nov. 2024), pp. 77–106. DOI: 10.47672/ajir.2523.

[2] *The 2025 Crypto Crime Report*. Unpublished report. 2025.

[3] W. Chen et al. “Misbehavior Detection on Blockchain Data”. In: 2021, pp. 95–133. DOI: 10.1007/978-981-16-0127-9_5.

[4] N. Mungoli. *Deciphering the Blockchain: A Comprehensive Analysis of Bitcoin’s Evolution, Adoption, and Future Implications*. http://arxiv.org/abs/2304.02655. Accessed: 2025-06-30. Apr. 2023.

[5] K. Gagneja et al. “Traceability of cryptocurrency transactions using blockchain analytics”. In: *International Journal of Computing and Digital Systems* 9.2 (2020), pp. 159–165. DOI: 10.12785/IJCDS/090202.

[6] S. A. Raza, M. Shaikh, and K. Tahira. “Cryptocurrency Investigations in Digital Forensics: Contemporary Challenges and Methodological Advances”. In: *Information Dynamics and Applications* 2.3 (Sept. 2023), pp. 126–134. DOI: 10.56578/ida020302.

[7] M. Z. Mas'ud et al. "A Review of Digital Forensics Framework for Blockchain in Cryptocurrency Technology". In: *2021 3rd International Cyber Resilience Conference (CRC)*. IEEE, 2021. DOI: 10.1109/CRC50527.2021.9392563.

[8] S. Salisu, V. Filipov, and B. Pene. "Blockchain Forensics: A Modern Approach to Investigating Cybercrime in the Age of Decentralisation". In: *Proceedings of the 18th International Conference on Cyber Warfare and Security*. Accessed: 2025-02-01. Towson, 2023, pp. 338–347. URL: https://papers.academicconferences.org/index.php/iccws/issue/view/16/18.

[9] Y. Wu et al. "A Bitcoin Transaction Network Analytic Method for Future Blockchain Forensic Investigation". In: *IEEE Transactions on Network Science and Engineering* 8.2 (Apr. 2021), pp. 1230–1241. DOI: 10.1109/TNSE.2020.2970113.

[10] S. Meiklejohn et al. "A fistful of bitcoins: Characterizing payments among men with no names". In: *Proceedings of the ACM SIGCOMM Internet Measurement Conference (IMC)*. 2013, pp. 127–139. DOI: 10.1145/2504730.2504747.

[11] P. Zheng et al. "On-chain and Off-chain Blockchain Data Collection". In: *Blockchain Intelligence: Methods, Applications and Challenges*. Springer Singapore, 2021, pp. 15–39. DOI: 10.1007/978-981-16-0127-9_2.

[12] A. hyun Park et al. "Forensic investigation framework for cryptocurrency wallet in the end device". In: *Computers & Security* 133 (Oct. 2023). DOI: 10.1016/j.cose.2023.103392.

[13] A. Holmes and W. J. Buchanan. "A framework for live host-based Bitcoin wallet forensics and triage". In: *Forensic Science International: Digital Investigation* 44 (Mar. 2023). DOI: 10.1016/j.fsidi.2022.301486.

[14] S. Taylor et al. "A comprehensive forensic preservation methodology for crypto wallets". In: *Forensic Science International: Digital Investigation* 42–43 (Oct. 2022). DOI: 10.1016/j.fsidi.2022.301477.

[15] W. Koerhuis, T. Kechadi, and N. A. Le-Khac. "Forensic analysis of privacy-oriented cryptocurrencies". In: *Forensic Science International: Digital Investigation* 33 (June 2020). DOI: 10.1016/j.fsidi.2019.200891.

[16] L. Infante et al. "Recovery CAT: A Digital Forensics Tool for Cryptocurrency Investigations". In: *12th International Symposium on Digital Forensics and Security (ISDFS 2024)*. IEEE, 2024. DOI: 10.1109/ISDFS60797.2024.10527279.

[17] K. Kent et al. *Special Publication 800-86: Guide to Integrating Forensic Techniques into Incident Response*. NIST Special Publication 800-86. Recommendations of the National Institute of Standards and Technology. National Institute of Standards and Technology (NIST), 2006. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf.

[18] Badan Standardisasi Nasional. *SNI ISO/IEC 27037:2014*. Pedoman identifikasi, pengumpulan, akuisisi dan pelestarian bukti digital. 2014.

[19] Badan Standardisasi Nasional. *SNI ISO/IEC 27042:2015 (diadopsi 2021)*. Pedoman analisis dan interpretasi bukti digital. 2021.

[20] A. R. Hakim et al. "A Novel Digital Forensic Framework for Data Breach Investigation". In: *IEEE Access* 11 (2023), pp. 42644–42659. DOI: 10.1109/ACCESS.2023.3270619.

[21] Weili Chen et al. "Misbehavior Detection on Blockchain Data". In: *Blockchain Intelligence: Methods, Applications and Challenges*. Ed. by Zibin Zheng and H.-N. Dai. Springer Singapore, 2021, pp. 95–133. DOI: 10.1007/978-981-16-0127-9_5.

[22] S. Kethineni and Y. Cao. "The Rise in Popularity of Cryptocurrency and Associated Criminal Activity". In: *International Criminal Justice Review* 30 (2019). DOI: 10.1177/1057567719827051.

[23] M. Alnasaa et al. *Crypto, Corruption, and Capital Controls: Cross-Country Correlations*. Tech. rep. WP/22/60. International Monetary Fund, Mar. 2022.

[24] A. Ibrahimi and B. Arifi. *Corruption and Cryptocurrency: Blockchains as Corruption Tools*. Unpublished manuscript. 2023.

[25] N. Hiramoto and Y. Tsuchiya. "Measuring dark web marketplaces via Bitcoin transactions: From birth to independence". In: *Forensic Science International: Digital Investigation* 35 (Dec. 2020). DOI: 10.1016/j.fsidi.2020.301086.

[26] M. Paquet-Clouston, B. Haslhofer, and B. Dupont. "Ransomware payments in the Bitcoin ecosystem". In: *Journal of Cybersecurity* 5.1 (2019), pp. 1–11. DOI: 10.1093/cybsec/tyz003.

[27] F. Najjar et al. "Change Address Detection in Bitcoin using Hierarchical Clustering". In: *Proceedings of the 2024 IEEE World Forum on Public Safety Technology (WFPST 2024)*. IEEE, 2024, pp. 42–48. DOI: 10.1109/WFPST58552.2024.00015.

[28] S. Salisu, V. Filipov, and B. Pene. *Blockchain Forensics: A Modern Approach to Investigating Cybercrime in the Age of Decentralisation*. Preprint or conference material. 2023.

[29] A. Yang. *Cryptocurrency Security Study based on Static Taint Analysis*. Unpublished work. 2023.

[30] *Virtual Assets and Virtual Asset Service Providers*. https://www.fatf-gafi.org. Accessed: 2025-06-30. 2019.

[31] *Best Practices for Search and Seizure of Electronic and Digital Evidence: Guidelines for Digital Forensics First Responders*. Published by INTERPOL or relevant agency. 2021.

[32] *Convention on Cybercrime*. Council of Europe, Budapest Convention. 2001.

[33] *International Standards on Combating Money Laundering and the Financing of Terrorism Proliferation: The FATF Recommendations*. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Fatfrecommendations.html. Accessed: 2025-06-30. 2012.