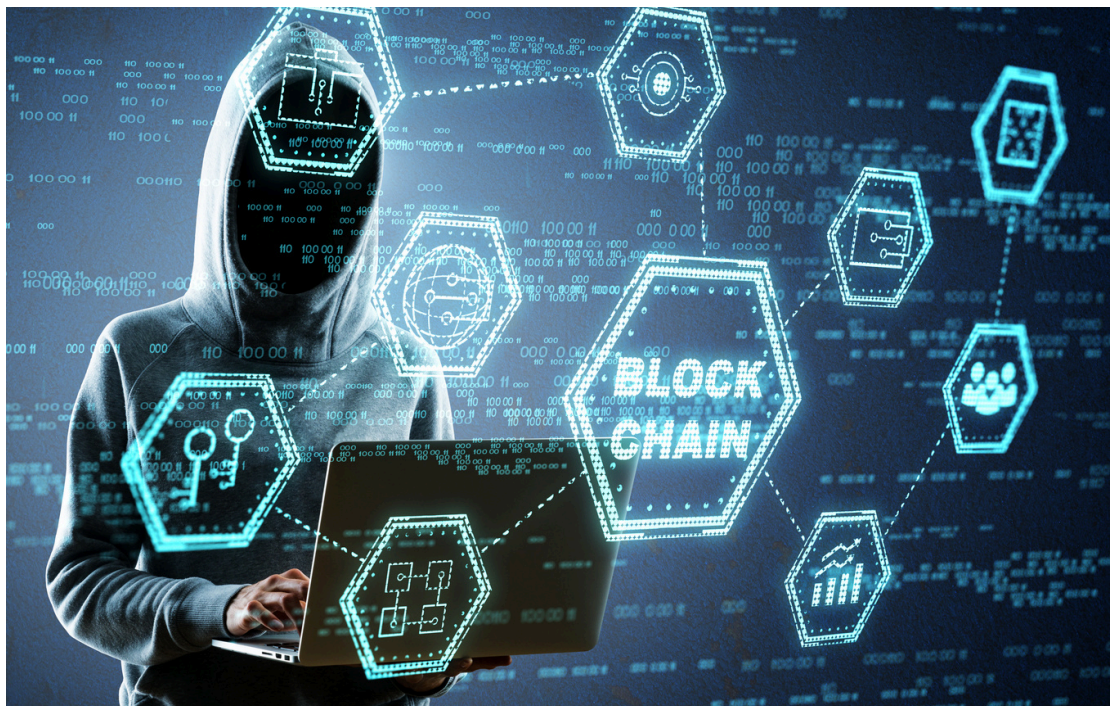
INVESTIGATING FINANCIAL CRIME IN CRYPTO ASSETS: BLOCKCHAIN FORENSICS

I. The Role of Blockchain Forensics in the Crypto Asset Ecosystem

Blockchain forensic analysis aims to trace fund flows, identify transaction patterns, and link crypto-asset activities to natural persons or legal entities through the systematic examination of transactions occurring on the blockchain. Unlike traditional financial forensic investigations, this discipline does not rely on centralized record-keeping systems but instead draws on transaction data maintained on decentralized and pseudonymous ledgers such as Bitcoin and Ethereum. In this context, blockchain forensics integrates on-chain data, including transaction histories, wallet addresses, and smart contracts, with off-chain data sources such as open-source intelligence, institutional records, and sanctions lists in order to determine the origin, destination, and contextual background of digital asset transfers.

With the widespread adoption of crypto assets and decentralized platforms, investigations into activities such as money laundering, illicit finance, fraud, and cybercrime increasingly rely on the discipline of blockchain forensics. While the inherent characteristics of blockchain technology, including transparency and immutability, present significant opportunities for investigators, the decentralized and anonymous or pseudonymous nature of transactions also makes such investigations more complex. For this reason, the objective is to enable the identification of real actors behind pseudonymous transaction systems by employing specialized tools and techniques such as on-chain analysis, heuristic assessments, and cross-verification with off-chain data in order to unravel complex transaction networks and trace digital asset movements across a global and distributed infrastructure.



II. Building Blocks of Forensic Analysis Reports

a) Core On-Chain Analytical Methods and Technical Tools

Blockchain intelligence tools are analytical systems that examine blockchain data in order to trace and understand crypto asset transactions. These tools analyze transaction histories, relationships between addresses, and on-chain interactions to detect suspicious activity and follow the flow of funds. By enabling the interpretation of complex and multi-layered transaction structures, they provide a foundation for linking blockchain activity to real-world individuals or entities. In this respect, blockchain intelligence tools constitute the technical backbone of forensic investigating reports.

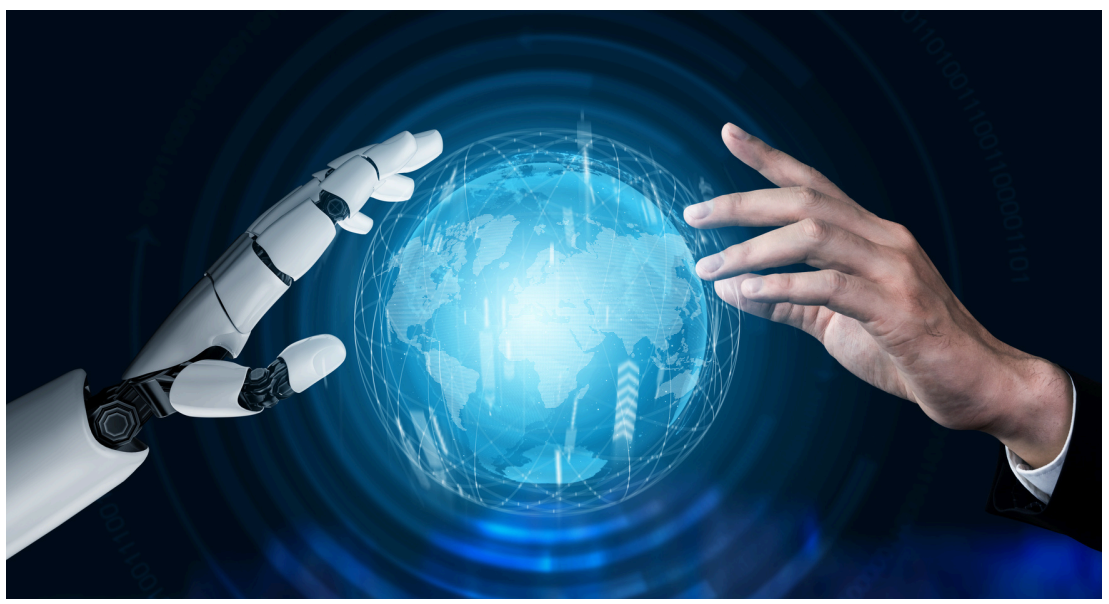
To effectively investigate crimes committed on the blockchain, forensic investigators employ multiple analytical methods in combination. In this context, the primary techniques include transaction analysis, address clustering, the use of blockchain explorers, taint analysis, and wallet identification. Each of these methods contributes to identifying the origin, movement, and ultimate destination of funds and is applied in a complementary manner.

Transaction analysis is one of the most fundamental techniques in blockchain forensics. Because blockchain transactions occur within a network composed of nodes, network analysis can be used to examine relationships between transactions and addresses. By analyzing factors such as the amount, frequency, and timing of individual transactions, as well as their links to addresses previously associated with illicit activity, investigators can identify transaction patterns that may indicate criminal conduct. These analyses are particularly useful for detecting high-value or repetitive transfers and fund movements concentrated around specific groups of addresses.

Address clustering, by contrast, seeks to assess whether separate wallet addresses visible on the blockchain are in fact controlled by the same individual or entity. Technical methods applied on the basis of indicators such as transaction graphs, the frequency of fund transfers, and similarities in transaction amounts are widely used, particularly on the Bitcoin network. Through this technique, addresses that regularly exchange funds with one another are grouped into the same cluster, making it possible to map fund flows within a broader framework. This mapping process, conducted through transaction graph analysis, reveals how funds are transferred from one wallet to another and enables the disentanglement of complex transaction chains.

Another critical element of forensic investigating from the perspective of technical verification and evidentiary integrity is the use of transaction hash values and timestamps. Each blockchain transaction is identified by a unique cryptographic hash that permanently links it to a specific block, thereby enabling verification of transaction integrity and chronological order and creating an immutable audit trail. Through blockchain explorers, investigators can quickly access transaction hash values, sender and recipient addresses, transferred amounts, and timestamp information, all of which play an important role in documenting investigative findings. In addition, taint analysis and wallet identification techniques make it possible to trace the on-chain movement of funds associated with illicit activity and to identify addresses that have come into contact with such funds.

In forensic investigation reports, a typology-based approach refers to the reconfiguration of analytical techniques in response to money laundering methods that deliberately seek to reduce the traceability of crypto assets. The use of mixers and tumblers, crypto asset swap transactions, chain hopping, and conversions carried out through decentralized protocols can render traditional address-based tracing methods largely ineffective. In such scenarios, forensic investigation shifts away from direct fund to address matching and instead relies on indirect tracing techniques based on transaction behavior, timing, value distribution, and network-level relationships. In these cases, forensic analysis focuses less on tracking funds on a one-to-one basis and more on examining temporal correlations between inbound and outbound transactions, similarities in transaction amounts, and clustering patterns across the network. The objective is not to follow individual units of value, but to identify the statistical and behavioral links between assets exiting a liquidity pool and prior illicit activity. Similarly, in crypto asset swaps and cross-chain transactions, investigative attention concentrates on transition points, bridge contracts, and moments of conversion. In such cases, the analysis aims to reveal recurring tracing patterns and points of contact with specific actors, rather than merely identifying the destination blockchain.



b) From On-Chain to Off-Chain: Attribution, Know Your Customer (*"KYC"*) Principles and Evidentiary Logic

Findings obtained through on-chain analysis reveal the technical footprint of crypto asset transactions. However, in order to link these activities to real individuals or entities, such findings must be supported by off-chain data. At this stage, associating wallet addresses with known individuals, entities, or platforms becomes possible through the use of KYC records, open-source intelligence, and technical analysis methods. Off-chain analysis encompasses the evaluation of transactions that occur outside the blockchain, which are typically maintained by crypto exchanges, intermediaries, or other market participants, and seeks to place on-chain information into a real world context by incorporating external data sets such as regulatory filings, social media data and dark web sources.

In off-chain compliance and investigative processes, analysts assess transaction orders, executed trades, deposit and withdrawal records, KYC submissions, customer due diligence data, and information relating to fiat currency to crypto asset on-ramps and off-ramps in combination. In this context, the synthesis of on-chain and off-chain data has become a fundamental method in both investigative and compliance workflows. For example, once a suspicious transaction pattern is identified through on-chain analysis, if the related funds are found to have interacted with a regulated exchange, KYC information may be requested from that platform in order to establish attribution. Similarly, compliance professionals can combine off-chain customer data with on-chain transaction analysis to submit reports with evidentiary value to regulatory authorities. This approach enables digital asset movements to be rendered verifiable and properly documented.

III. From Tracing to Intervention: Sanctions, Freezing and Asset Recovery

The use of crypto assets in corruption, fraud, and illicit finance requires forensic investigative efforts to extend beyond the detection phase and to incorporate effective intervention and asset recovery mechanisms. Traditional asset seizure and freezing regimes are largely designed around bank accounts or tangible assets, and the cross-border, instantaneous, and decentralized nature of crypto assets places significant challenge on these frameworks. The ability to transfer crypto assets rapidly without direct government oversight complicates coordination in cases involving multiple jurisdictions. As a result, it has become increasingly important to deploy legal and technical intervention tools in parallel with asset tracing. Recent enforcement practice demonstrates that crypto asset recovery does not rely on tracing alone, but rather on the combined use of blockchain analytics, judicial seizure mechanisms, and issuer-level technical controls.

In practice, sanction and intervention processes targeting digital assets are carried out through distinct but interrelated mechanisms. Seizure refers to the transfer of control over digital assets to public authorities pursuant to a court order and, in most cases, involves instructing exchanges, custodial service providers, or issuers to transfer the assets to government-controlled wallets.

Freezing or blocking, by contrast, seeks to restrict the movement of an asset without removing it from the blockchain and is typically implemented by issuers, smart contracts, or custodial platforms. Burning refers to the permanent removal of tokens from circulation by sending them to an irrecoverable address, while reissuance is a technical practice that enables the issuance of equivalent tokens to government-controlled wallets or to victims in an amount corresponding to the burned or frozen funds. Forfeiture, in turn, is a legal mechanism through which ownership of assets determined to be connected to criminal activity is permanently transferred to the state and may be pursued through criminal proceedings.

An illustrative example of how these mechanisms operate in practice is the civil seizure action filed on June 18, 2025, by the United States Attorney's Office for the District of Columbia. In that case, the seizure of more than USD 225 million in crypto assets was sought after the assets were determined to be linked to a large-scale international investment fraud scheme, marking the largest crypto asset seizure connected to investment fraud in United States history. In the investigation conducted by the U.S. Secret Service and the FBI, blockchain analytics were used to trace illicit funds through peel chain structures, intermediary wallets, cross-chain transfers, and consolidation addresses, and once the funds were linked to identifiable wallets and regulated platforms, legal seizure became possible.

IV. Challenges in Blockchain Forensics

Although blockchain forensics has become an increasingly effective tool in the investigation of illicit transactions, fraud, and other crimes involving crypto assets, it faces significant structural and technical challenges. One of the primary challenges is the lack of data standardization across blockchains. The fact that each blockchain has its own data structures, transaction formats, and technical characteristics makes cross-chain analysis and comparison difficult, particularly in cases involving multiple blockchains, which further complicates tracing efforts. Moreover, even though blockchain data is publicly available, the need to analyze a large number of wallet addresses and transactions in each case, reconstruct fund flows accurately, and properly interpret findings requires substantial time, technical capacity, and specialized expertise.

In addition, inherent features of blockchain technology such as decentralization, pseudonymity, and the irreversibility of transactions create a favorable environment for actors seeking to deliberately reduce traceability. The fact that crypto wallets are often anonymous and cannot be directly controlled by a central authority limits the effectiveness of traditional legal tools. The rapid movement of funds across different networks and addresses through mixers and tumblers, cross-chain transactions, decentralized exchanges, and privacy-focused crypto assets further complicates direct fund tracing. Moreover, techniques such as splitting transactions into numerous small amounts, rapidly circulating funds across multiple wallets, or converting assets into NFTs (*Non-Fungible Token*) or stablecoins make transaction patterns increasingly complex. These technical challenges necessitate that on-chain findings be supported by KYC records and other off-chain data; however, the reliability of such data and the fact that legal frameworks have not yet fully matured introduce additional uncertainty into investigative and compliance processes. As a result, the effectiveness of blockchain forensics depends not only on technical analytical capabilities, but also on inter-institutional cooperation and multi-layered data integration.