BLOCKCHAIN INTELLIGENCE GROUP

DIGITAL DETECTIVES

A Step-By-Step Guide For Cryptocurrency Investigations For Law Enforcement

January 2025

Developed in Partnership with The Block Audit

Introduction

This guide is designed to equip law enforcement officers with essential knowledge and practical tools for investigating cryptocurrency-related crimes. This resource will simplify complex concepts and provide actionable guidance.

Procedures and best practices for handling each stage of your investigation are described, in addition to a simple step-by-step guide for cryptocurrency investigations. This resource also includes our contact information so you can get in touch with us if you need any additional help or professional support. Please do not hesitate to reach out.

Chapter 1: Understanding Cryptocurrencies

What is Cryptocurrency?

Cryptocurrency is a digital or virtual form of value (like fiat currency) that uses cryptography for security. Unlike traditional currencies governments issue, cryptocurrencies operate on decentralized networks based on blockchain technology.

Common Cryptocurrencies

- **Bitcoin**: The first and most well-known cryptocurrency, often called digital gold.
- **Ethereum**: Known for its smart contract functionality, enabling decentralized applications (DApps).
- **Altcoins**: Other cryptocurrencies like Litecoin, Ripple, and others, each with unique features.
- **Stablecoins**: Cryptocurrencies designed to maintain a stable value by being pegged to a reserve asset, like the US dollar, reducing volatility.

Blockchain Technology

Definition: A blockchain is a distributed ledger that records all transactions across a network of computers.

In Plain English

A blockchain functions similarly to a digital database, which is shared by multiple computers (nodes). These nodes are operated by individuals or entities globally and work together to keep the blockchain secure and reliable. Every transaction is recorded in this database and is visible to all. This is referred to as a distributed ledger and ensures that everyone has the

same copy of the transaction records, allowing all transactions to be easily verified. Once a transaction is entered into the database or digital ledger, it cannot be changed or erased.

Anonymity and Pseudonymity

One of the key characteristics of cryptocurrencies is their potential for anonymity and pseudonymity. This can be a challenge, particularly when conducting investigations.

Anonymity: A common misconception about cryptocurrencies is that they are anonymous. However, true anonymity is rare. Most cryptocurrencies do not offer complete anonymity, but some, like Monero and Zcash, have been designed to enhance privacy and make it very difficult to trace transactions back to individuals.

Pseudonymity: Most cryptocurrencies, including Bitcoin and Ethereum, are pseudonymous rather than anonymous. This means that while transactions are publicly recorded on the blockchain, the identities of the parties involved are not directly tied to their public keys (addresses). Instead, users are identified by their wallet addresses, which can be linked to their real identities through various means, such as exchange KYC (Know Your Customer) requirements and transaction patterns.

Chapter 2: Crime in Crypto

Utilizing the unique qualities of blockchain technology and cryptocurrency transactions, bad actors have quickly turned to using cryptocurrencies for a wide range of illicit activities. Perpetrators weaponize anonymity, target users with false investment prospects, and exploit their victims' emotional vulnerabilities through romance scams.

Criminals leverage cryptocurrencies to obfuscate the origins of funds obtained through a range of illicit activities. Some of the most common crypto-based crimes include:

Laundering funds from Illicit Sources

Cryptocurrencies provide several instruments for money laundering:

- **Mixing Services:** These services combine cryptocurrencies from several sources, making it almost impossible to determine who originally owned the money.
- **Tumbling:** Breaking down significant transactions into several smaller, seemingly unconnected ones is known as "tumbling," it further obfuscates the chain of transactions.
- **Chain Hopping:** Using the different degrees of anonymity each blockchain provides, criminals move money between them.

Investment Fraud

Investment Fraud includes a wide range of schemes to target naive individuals to invest in fake or misleading cryptocurrency projects. There are three main types:

- **Initial Coin Offering (ICO) Scams:** Similar to a traditional initial public offering in the financial markets, scammers create a new cryptocurrency and start an ICO, promising big profits and cutting-edge technology. They often create realistic marketing materials and white papers (technical documents) to look authentic. At times, the project might not even actually exist. The people who invest money end up buying worthless tokens and lose their money to con artists who take the money and run.
- **Ponzi Schemes:** Ponzi schemes are pyramid schemes that use money from new investors to pay back money promised to investors who invested earlier. Fraudsters make a fake cryptocurrency or investment platform and promise investors high returns. Initial payouts are made with money from later investors, giving the impression of success. Ultimately, the scheme fails because it's not possible to get enough new investors to keep paying out the money.
- **Romance Scams**: Often referred to as pig butchering scams, in these scams, fraudsters use dating apps and social media platforms to establish romantic relationships with their victims. Once trust is built, the scammer will fabricate a

financial emergency or propose an investment opportunity, persuading the victim to send cryptocurrency. The scammer then vanishes, leaving the victim heartbroken and financially devastated.

Ransomware Attacks

Cybercriminals use harmful software called ransomware to encrypt their victims' computer files, making them impossible to access. Then, they ask for a ransom, usually paid in cryptocurrency, to unlock the files. The anonymity of cryptocurrency makes it appealing to hackers because it's difficult for police to track ransom payments. People, businesses, and even critical infrastructure are the targets of these attacks, which cause a lot of headaches and steep financial losses.

Transactions on the Dark Web

The dark web is a part of the internet where people can browse anonymously and buy and sell illegal goods and services. Cryptocurrencies are often used to pay in these markets because they are pseudo-anonymous and make sending money across borders easy. Some common types of dark web marketplaces where cryptocurrency transactions occur include:

- **Drug trafficking**
- **Guns and Weapons**
- **Financial accounts (credit cards, bank accounts, passwords)**
- **Child Sexual Abuse Material (CSAM)**

Malware Attacks

There are several ways that malicious software (malware) can attack people who use cryptocurrencies:

- **Crypto Theft:** Keyloggers and other types of malware can steal login information and private keys, which lets thieves get into victims' wallets and steal cryptocurrency directly from them.
- **Cryptojacking:** This crime involves malware that uses a person's computer to "mine" cryptocurrency for the attacker's own gain. This can make the victim's computer run much more slowly and increase their electricity costs.

Phishing Scams

A type of scam where attackers trick individuals into revealing sensitive information like private keys or recovery phrases for their cryptocurrency wallets or trick users into giving permission to withdraw tokens from their wallet.

This is done using the following methods:

- **Fake/Malicious Apps**: Scammers create applications that mimic legitimate crypto wallets or exchanges to steal login credentials.
- **Impersonation**: Attackers pose as representatives from trusted entities to gain trust and extract sensitive information.
- **Misleading Links**: Emails, messages or social media posts with links leading to fraudulent websites designed to look like authentic platforms. The user is prompted to connect their wallet and is then tricked into giving permission to withdraw tokens from their wallets.

Giveaway Scams

Crypto giveaway scams are fraudulent schemes where scammers promise to give away a significant amount of cryptocurrency in return for a smaller amount sent to them or for personal information. Here is how they work.

- These scams often exploit the names and reputations of well-known figures or companies to create a sense of legitimacy and urgency.

- Scammers use sophisticated phishing websites that mimic legitimate cryptocurrency brand promotions, complete with stolen branding elements and images.
- The scam begins with enticing advertisements or social media posts claiming a large sum of money is being given away, often using clickbait headlines to attract attention.
- Victims are directed to send a certain amount of cryptocurrency to a wallet address controlled by the scammers with the false promise of receiving a larger amount in return.
- No actual giveaway occurs; instead, the scammers steal the funds sent by the victims.
- These scams prey on human emotions such as greed and the fear of missing out (FOMO), leading to significant financial losses for the victims.

Impersonation Scam

Scammers employ a variety of tactics to convince victims to willfully convert their fiat currency held in traditional financial institutions into cryptocurrency. This is often "on-ramped" into the scammer's direct control. This is accomplished by either having the victim purchase and send cryptocurrency through a crypto kiosk (Bitcoin ATM), or by the scammers facilitating the creation of legitimate VASP accounts in the name of the victim, but where the scammers have total control of the account. This scam may take multiple forms:

- Victim receives a call from someone claiming to be a police officer, who informs them they missed a court date for jury duty. As a result, an arrest warrant has been issued, but it can be cleared by paying an administrative fee through a crypto kiosk.
- Victim receives a call from a person claiming to be an IRS agent who states there was a mistake on taxes and they need to pay the balance immediately to avoid being arrested.
- Victim receives a call from an attorney stating that a family member (often a grandchild) was at fault in a car accident and seriously injured a pregnant woman. The family member is facing serious charges but the attorney states he can represent the family member and get them off, or otherwise pay bail, or settle with the supposed victim. The "attorney" requires immediate payment via crypto kiosk.
- A fast food restaurant receives a call from someone representing themselves as the district manager. The "district manager" states that an unexpected inspector from the corporate office is on the way to the store to conduct an audit. The manager

states that he needs the employee to take all of the cash out of the drawers and deposit into a crypto kiosk so that they do not fail the audit.

- The victim receives a call from who they believe to be their bank representative. The bank representative explains that they have a dirty employee who has been stealing from customers. That employee has now targeted the victim's account. In order to protect their money while also allowing the bank representative to catch the bad employee, the victim is directed to withdraw and then deposit all of their funds into a crypto kiosk.

Chapter 3: Identifying and Analyzing Cryptocurrency

Although cryptocurrencies provide greater privacy than traditional currencies, the ledger (decentralized database) on which transactions are verified and recorded is public for most blockchains. Therefore, investigators may theoretically track every transaction back to its source.

Identifying Wallets and Addresses

It is essential to remember that while cryptocurrency transactions don't use real names, they are not wholly anonymous. A crypto wallet is like a digital bank account that keeps track of credit. Like an account number, each wallet has its address, which you can send and receive cryptocurrency to and from. Information about the address, including its transactional history, account balance, and other details are publicly available.

Cryptocurrency addresses also use different formats depending on the cryptocurrency. While all cryptocurrencies use a blockchain, the addresses differ in format.

Cryptocurrency Address Examples:

Bitcoin addresses begin in a 1, 3, or bc1.

Examples:

1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

3J98t1WpEZ73CNmQviecrnyiWrnqRhWNLy

bc1qar0srrr7xfkvy5l643lydnw9re59gtzzwf3dl

Ethereum addresses begin with an 0x.

Example: [0xde0B295669a9FD93d5F28D9Ec85E40f4cb697BAe]

Tron addresses begin with a T.

Example: [TQ5NRbu7etZ6uxwDQLF7kZJoQ38vdNWjci]

Identifying Cryptocurrency in the Field

It's possible for law enforcement to come across important giveaways in the field which may indicate that cryptocurrency is involved. In the field, keep an eye out for the following:

Seed Phrases

Often written on a piece of paper, a seed phrase, also known as a recovery phrase or mnemonic phrase, is a sequence of typically 12 to 24 words randomly generated by a cryptocurrency wallet. The phrase serves as a backup that allows users to access their funds in case their device is lost, stolen or damaged.

Cryptocurrency ATM Receipts

ATM receipts can be either paper receipts or digital receipts sent via text message or email. They typically include the transaction date, the amount of cryptocurrency purchased and the deposit address. The exact format and details may vary depending on the ATM provider.

Crypto Wallets

1. **Hardware Wallets**: Look for small physical devices similar to USB drives. Common brands include Ledger and Trezor. These devices will often come with a cable for connecting to a computer.
2. **Software Wallets**:
    - **Desktop Wallets**: Check the suspect's computer for installed programs related to cryptocurrencies, such as Electrum or Exodus. These can usually be found in the applications or programs folder.
    - **Mobile Wallets**: Inspect smartphones for cryptocurrency apps like Trust Wallet or Mycelium. Look for these in the app drawer or home screen.
3. **Web Wallets**: Look through internet browser history or bookmarks for access to online wallets. Common websites include Coinbase and Blockchain.info. Also, check for saved login credentials in the browser's password manager.
4. **Paper Wallets**: These are physical pieces of paper with printed keys and QR codes. They might be stored in safes, files, or personal belongings. Look for documents with long strings of letters and numbers or QR codes.
5. **Cold Wallets**: Any offline storage method. This includes both hardware and paper wallets. When investigating, any device or document not connected to the internet that holds keys could be considered a cold wallet.
6. **Hot Wallets**: Connected to the internet for frequent use. These include software wallets on computers and smartphones, as well as web wallets. Look for evidence of frequent transactions or online activity related to cryptocurrency.

Chapter 4: Investigative Tools

Investigating cryptocurrency-related crimes requires an understanding of the tools and techniques available to trace transactions and uncover illicit activities. This section explores

various tools and methodologies that law enforcement officers can use during their investigations.

The goal in conducting a cryptocurrency tracing investigation is to follow the flow of funds across the blockchain until it reaches an entity, like an exchange, that collects KYC information.

Blockchain Explorers

Blockchain Explorers are web-based tools that allow users to search and view transactions on blockchains. They are essential for tracing cryptocurrency movement and identifying end-points.

- **Blockchain.com:** This explorer is commonly used to track Bitcoin transactions. It provides detailed information about transaction histories, including addresses, transaction amounts, and timestamps.
- **Etherscan.io:** Specifically designed for the Ethereum blockchain, Etherscan allows investigators to track Ethereum transactions, view smart contracts, and analyze token transfers. It is crucial for investigating activities involving decentralized applications (DApps) and ERC-20 tokens.

Asset Tracing Methodologies

As you begin to follow the flow of assets through various wallet addresses, it will quickly become apparent that assets become divided and commingled with other transactions which make it challenging to articulate the character of the assets as they progress through the money laundering process. While case law may vary by jurisdiction and is largely still non-existent in most courts as applied to cryptocurrency, there are general principles of asset tracing that may be applied to assist in articulating the flow of funds. The successful application of these techniques may rely on the investigator's qualifications and justifications of their application, but are described below for reference.

- Proceeds-In-First-Out (PIFO)- This method treats all existing assets in a wallet prior to the illicit transfer as legitimately owned by the wallet owner. Once the illicit assets

enter the wallet, the owner will want to enter those assets into the layering stage of the money laundering process as soon as possible. For this reason, despite any additional deposits which enter the wallet after the illicit assets, all outbound transactions will be ascribed to the illicit assets up until the amount of the original illicit deposit is disposed of. This is the most efficient method for following crypto assets through multiple wallet addresses.

- Lowest Intermediate Balance Rule (LIBR)- This method assumes that the wallet owner does not have the legal authority to transfer the title of illicit assets. For this reason, no matter how many transfers in or out occur within the wallet, so long as the lowest balance of the wallet never falls below the value of the illicit deposit, then the illicit funds remain inside the original wallet. This method is useful in restricting the movement of assets and may be best suited for claiming value held in cold wallets.
- Last-In-First Out (LIFO) - This method states that the last deposits in, are always the first to go out (like dealing from the top of a deck of cards). This method originates from inventory accounting practices and may become overly complicated in wallets with a large number of incoming and outgoing transactions.
- First-In-First Out (FIFO) - This method originates from inventory accounting and works in the opposite way from LIFO. This method states that the first assets to enter the wallet must be completely accounted for as leaving prior to reaching the illicit assets (like dealing from the bottom of a deck of cards). This method is also overly complicated when applied to cryptocurrency transactions.

Matching Transactions - This principle allows for deviation from any of the above listed methods. When a wallet has a specifically identifiable amount deposited, and that same specific amount is sent out within a short time, this method assumes that despite any other incoming or outgoing transactions, that the specific amount maintained its nature as the illicit funds (Ex. $1,666.41 in followed within 24 hours by $1,666.41 out). This method should be used sparingly and with clear articulation for the deviation.

Forensic Tools

Forensic tools are specialized software designed to analyze blockchain data, trace transactions, and uncover hidden connections. They are powerful allies in the fight against crypto crime.

QLUE™: is a comprehensive forensic tool developed by Blockchain Intelligence Group. QLUE™ is designed specifically for law enforcement agencies to assist in cryptocurrency investigations by providing detailed transaction analysis, visualization, monitoring, and reporting capabilities. By following the flow of funds using QLUE, investigators can oftentimes trace the funds to an exchange or entity that collects customer identifying information.

Key features include:

- **Visualization Tools:** QLUE™ includes powerful visualization tools that transform complex data into easy-to-understand graphs (pictured below). These visuals help investigators quickly grasp the flow of funds and identify key points of interest in their investigations.
- **Advanced Search Capabilities:** Investigators can perform detailed searches using various parameters, such as address, transaction hash, and amount, to pinpoint specific transactions and related entities.
- **Real-Time Tracking:** QLUE™ provides real-time tracking of cryptocurrency transactions, allowing investigators to monitor the movement of funds as it happens. This immediate insight is crucial for staying ahead of cybercriminals who might otherwise disappear with illicit gains.
- **Cross-Chain Investigations:** Criminals frequently employ a technique known as chain hopping in an attempt to break the connection between the source of funds and the final destination. QLUE™'s cross-chain investigation capabilities allow law enforcement to track assets across different blockchains, providing a holistic view of criminal networks and transactions.
- **Address Watch**: Address Watch allows users to monitor specific blockchain addresses in real-time. Investigators can set alerts for any suspicious activity associated with these addresses, facilitating proactive monitoring and intervention.

- **Exporting:** QLUE™ generates comprehensive, detailed transaction histories, visualizations, and data analyses that can be used in legal proceedings.

OSINT Tools

Open-source intelligence (OSINT) tools gather data analysis information from the internet to supplement traditional investigative techniques. These tools can provide valuable context and additional data points for cryptocurrency investigations.

Chapter 5: Legal and Procedural Considerations

The goal of tracing the flow of cryptocurrency across the blockchain is to follow the funds to an entity. Cooperative entities, or off-ramps, will provide investigators with the customer identifying information of who received the stolen or illicit funds.

KYC and AML Regulations

Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations are federal and state requirements that financial institutions, including cryptocurrency exchanges and crypto ATM providers, must adhere to. These institutions must verify customers' identities and monitor transactions for suspicious activity. Since financial institutions must adhere to these requirements, a law enforcement officer can obtain this data to further an investigation by issuing a valid subpoena to these organizations. You should seek agency policy or the direction of your prosecutor before requesting information via a subpoena.

- **KYC Information:** Exchanges collect KYC information such as customer names, addresses, identification documents, and photos. This data can help link cryptocurrency addresses to real-world identities.
- **AML Reporting:** Exchanges are required to report suspicious activities and transactions that exceed certain thresholds. Accessing these reports can alert investigators to potential money laundering schemes and other illicit activities.

Subpoenas and Legal Discovery

Subpoenas are legal documents that compel individuals or entities to provide testimony or produce evidence, such as documents or records. In the context of cryptocurrency investigations, subpoenas are essential tools for obtaining information from cryptocurrency exchanges, wallet providers, and other relevant entities.

- **Issuing Subpoenas:** Law enforcement agencies should follow their local policies for issuing subpoenas. .
- **Targeting Exchanges:** Cryptocurrency exchanges often hold valuable information, such as customer identification data, transaction histories, and IP addresses. Subpoenas can compel exchanges to provide this information, which is critical for linking transactions to individuals or entities.

Key Data Points to Subpoena

It is useful to know and understand which data an exchange or other crypto business can provide before issuing a subpoena. In general, most cryptocurrency exchanges and

businesses in the United States and Canada will be able to provide you with the following information:

- Activity / IP address log and multi-factor authentication device log
- Onboarding information and/or ID/selfie photo along verification report
- In case of an institution: incorporation documents, beneficial ownership additional business information and other documents specific to the entity type
- Transactions History: Deposits and Withdrawals (usually includes hashes and wallet addresses)
- Communication records: Emails, Phone calls, Support tickets, etc.

Contacting Exchanges or other Crypto Businesses (VASPs)

Businesses inside your jurisdiction will likely respond to your subpoena and cooperate. Many cryptocurrency businesses outside of your jurisdiction around the globe are increasingly complying with law enforcement requests voluntarily despite being outside the jurisdiction of a common court authority. These businesses may provide records in response to an official law enforcement letterhead request that they would on a subpoena. Each business may have their own requirements for verification or submission (a current list of VASP compliance is maintained at www.theblockaudit.com/legal-guide). Other cryptocurrency businesses may not respond or refer you to a mutual legal assistance process. This will likely take a minimum of six months. Communication directly with the jurisdiction's Financial Intelligence Unit may speed up the process.

Always remember to identify:

- The jurisdiction the business is located
- Regulatory or licensing status
- Contact e-mail address
    - info@[name].com

- cs@[name].com
- compliance@[name].com
- aml@[name].com
- pr@[name].com
- Social media (i.e., Linkedin) profile of the business' representatives

How To Handle Cryptocurrency Evidence

How is Cryptocurrency Seized?

1. Physical Devices

Once an enforcement action is undertaken and a seizure is likely, law enforcement officers should consider moving any cryptocurrencies quickly to an agency owned wallet. It should be noted that the cryptocurrency value does not exist in or on the seized device, but on the blockchain itself. Physical devices are only one way to access that value, so despite restricting physical access to the seized device, the value may still be drained from the wallet address to be seized if the suspect has additional means to access their private keys.

2. Exchange Accounts (VASPs)

Assets held in exchange accounts are not controlled by the target of an investigation, but are controlled by the Virtual Asset Service Provider on behalf of the target. These VASPs operate much like a traditional bank. They may be served with a seizure warrant just as a traditional bank to take custody of assets held in the name of your target. There are many VASPs around the globe that, despite being outside your home jurisdiction, will voluntarily comply with

seizure warrants and transfer custody of target assets to a law enforcement controlled wallet.

Identification

Learn about the various service providers for different types of crypto wallets, such as web, mobile, and computer-based wallets. There is frequently a time limit on accessing the suspect's crypto wallet once it is established that crypto is being used for illegal purposes.

Find out if the device's passcode or key can be obtained, as well as the crypto wallet. To stop tampering, limit access to any devices that might contain evidence.

Collection

Put the device in airplane mode or place it in a Faraday bag to stop tampering if you are unable to immediately access the suspect's crypto wallet.

Move the money to your department's wallet as soon as the suspect's computer or mobile device's wallet has been decrypted. To transfer money, enter the wallet address or scan the QR code, then push or click the transfer button. Examine all of the program's tabs and subfolders carefully because a crypto wallet might have several files that store crypto in different locations.

Preservation

Adhere to chain of custody and digital evidence handling procedures after transferring cryptocurrency to the departmental wallet. Verify whether the departmental wallet permits

the creation of a crypto vault, a security measure that necessitates two parties to approve a transfer.

Numerous providers of virtual wallets offer support for inquiries and investigations by law enforcement.

Investigative Use

The dark web makes frequent use of cryptocurrency. Crypto that has been seized might have been a part of a dark web market transaction. The blockchain database may provide important information for an investigation and works similarly to a complete history of bank transactions.

It is frequently possible to identify more suspects and organizations by following the money trail.

Chapter 6: Case Studies and Practical Examples

According to a recent Federal Bureau of Investigation (FBI) report, losses from cryptocurrency investment scams in the United States were $3.94 billion in 2023, up 53% from $2.57 billion in 2022. The losses are likely substantially higher due to non-reporting victims.

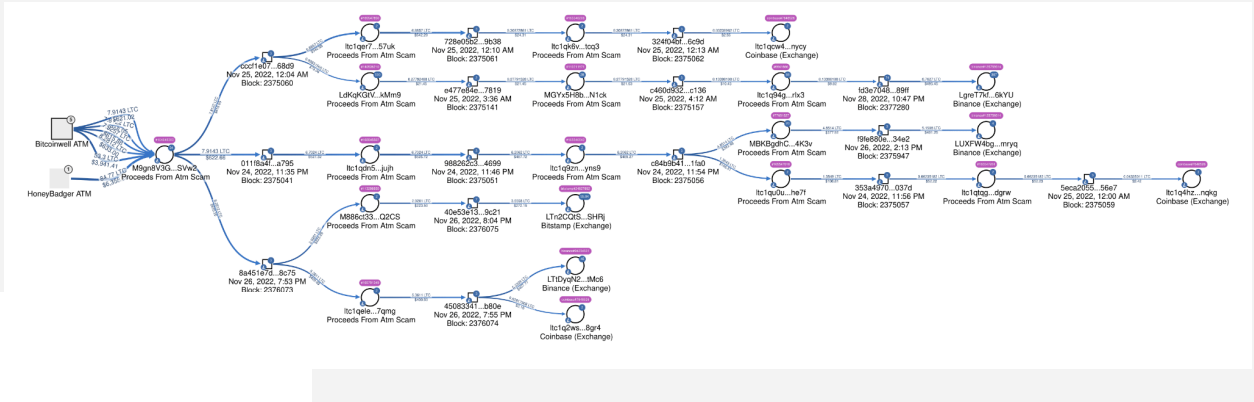
ATM Scam

This example examines an investigation conducted by Blockchain Intelligence Group into a cryptocurrency ATM scam involving Bitcoin and Litecoin transactions. The investigation aimed to identify the scammers and help recover the victim's funds.

In this case, the victim was conned by a very clever romance scammer. By creating a fake social media profile, the scammer tricked the victim into entering into an online relationship. The scammer then took advantage of the victim's vulnerable emotional state to create a false financial emergency, manipulating the victim into sending the money and promising to pay them back.

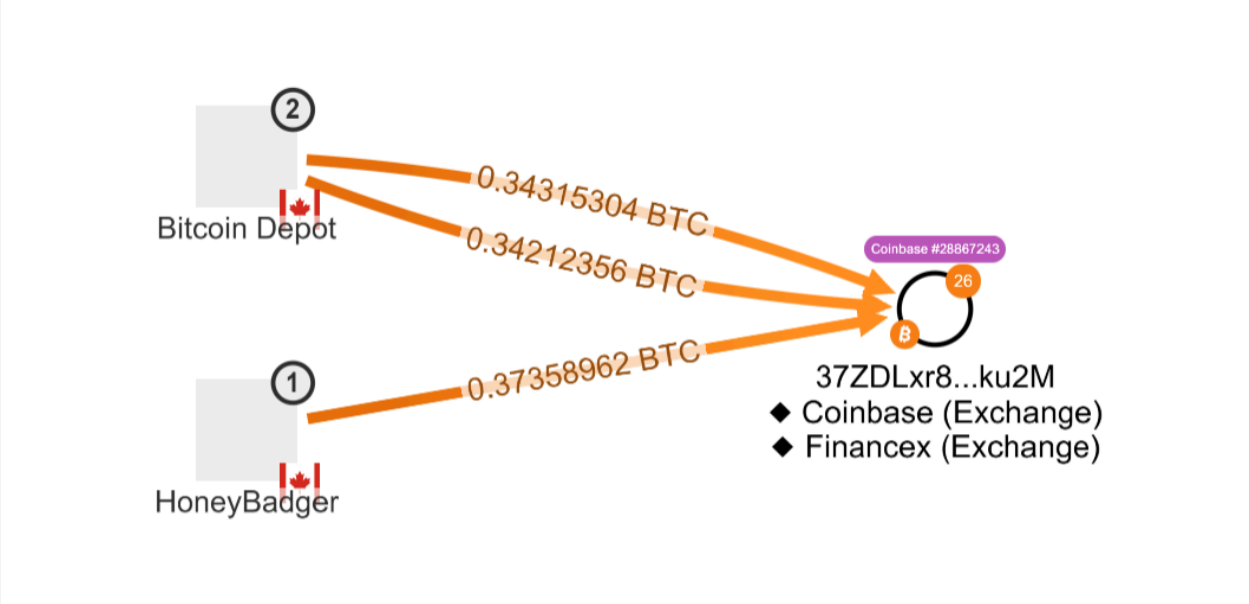
Litecoin Investigation

Between November 24 and November 27, 2022, the victim transferred around 170 Litecoin (LTC) via cryptocurrency ATMs. The investigation team tracked the funds sent to Litecoin withdrawal addresses based on the transaction receipts provided by the victim. When tracking these funds forward using QLUE™ it was found that a portion of these funds were sent to deposit addresses associated with major exchanges such as Binance, Bitstamp, and Coinbase in several hops (transactions).



Bitcoin Investigation

On November 28 and November 29, 2022, the victim conducted multiple Bitcoin transactions via 2 cryptocurrency ATMs, transferring approximately 1 BTC in total. Unlike the Litecoin side of the investigation, the Bitcoin transfers were all sent directly to a single customer deposit address at Coinbase exchange.

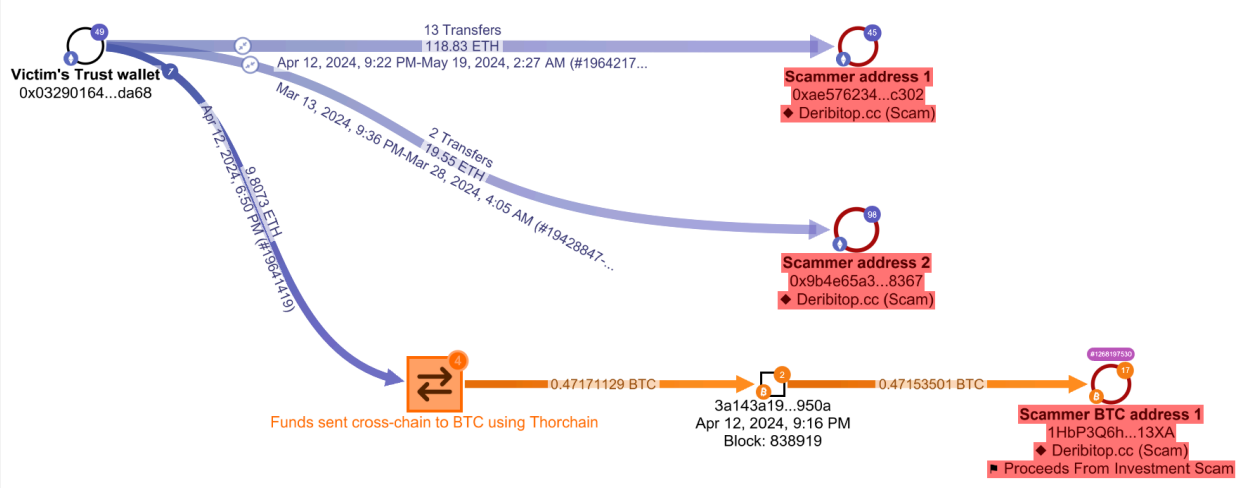


Most exchanges require users to undergo KYC (Know Your Customer) procedures, which could potentially link the deposit addresses to real-world identities of the scammers. By identifying these deposit addresses, investigators gained crucial leads that could help in pinpointing the individuals or entities behind the scam.

Pig Butchering Scam

Initial Investigation:

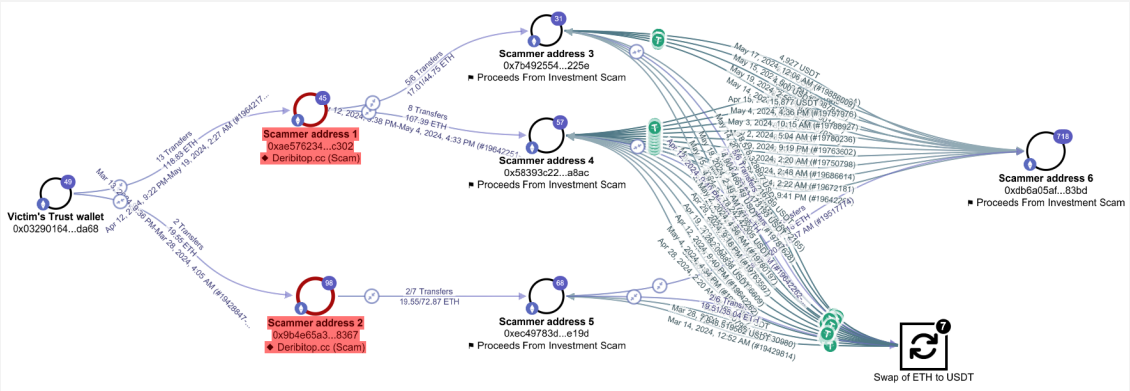
The victim was contacted and persuaded to invest in a fraudulent platform called Deribitop.cc. Following the scammer's instructions, the victim transferred money from their bank to Kraken, a cryptocurrency exchange. From Kraken, the victim transferred the funds to their Trust Wallet and sent them to 3 deposit addresses associated with the fraudulent platform. These addresses are labeled as Scammer addresses 1 and 2 and Scammer BTC address 1 on the graph. The victim sent these funds in 16 transactions between March to May 2024:



Ethereum

The investigation tracked the funds sent from the Scammer's Ethereum addresses forward. The addresses that received money from the victim were linked to a broader network of scammer addresses. Among these, a consolidation address emerged; this address could potentially be linked to other victims of the same scam.

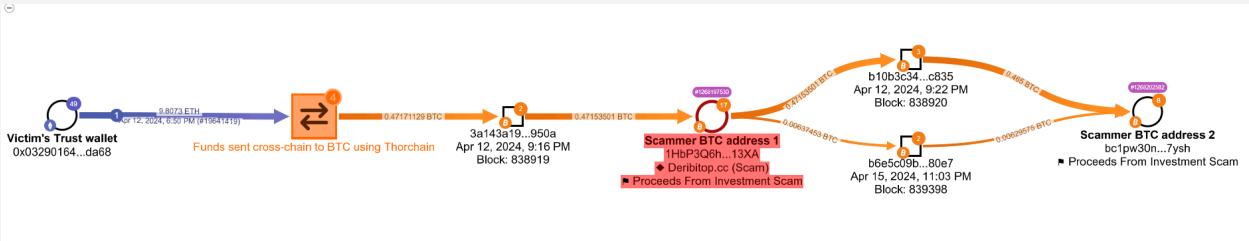
The funds from Scammer address 1 were sent to 2 intermediary addresses and converted to USDT and then sent to Scammer Address 6, similarly ETH from Scammer address 2 was sent to an intermediary address and to Scammer address 6 soon after.



These funds along with other funds from Scammer address 6 were then moved to several intermediary addresses before being deposited into exchange deposit addresses.

Bitcoin

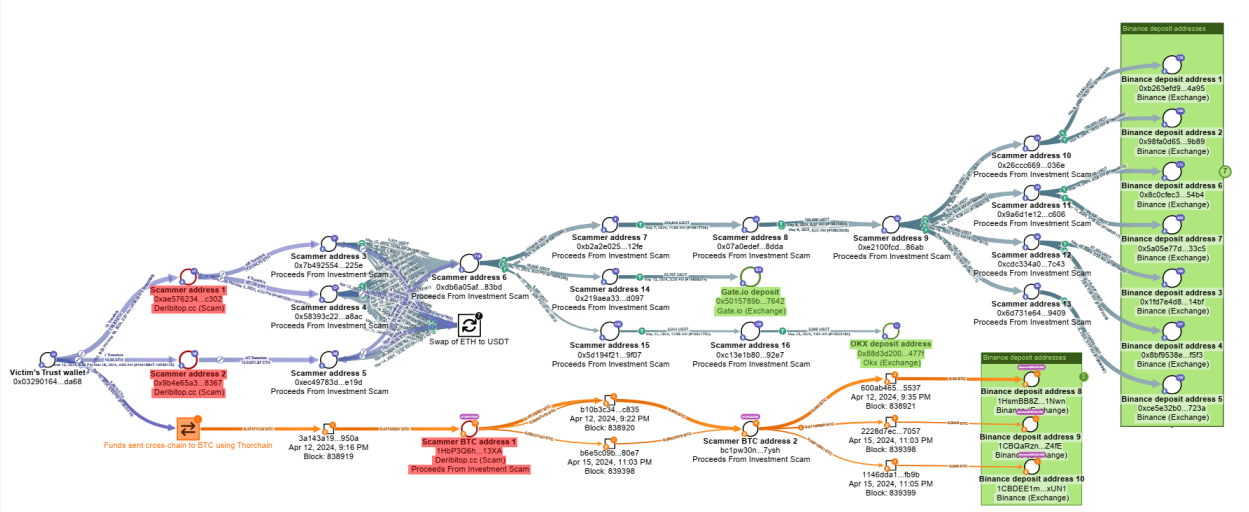
Funds sent to Scammer's Bitcoin address by the victim were then transferred to an intermediary address after which most of the funds were transferred to multiple exchange deposit addresses.



Reaching the Final Destination - Exchange Deposit Addresses:

The investigation revealed that the majority of the funds stolen from the victim appears to have eventually ended up in deposit addresses of various cryptocurrency exchanges, including Gate.io, OKX, and Binance. The exchange deposit addresses on the graph are highlighted in green.

These exchanges require users to undergo KYC (Know Your Customer) procedures, which could potentially link the deposit addresses to real-world identities of the scammers. By identifying these deposit addresses, investigators gained crucial leads that could help in pinpointing the individuals or entities behind the scam.



While this investigation can look overwhelming, with some basic training, it is relatively straightforward to conduct similar investigations in QLUE. If you would like to try, or see examples of how other cases have been graphed, please contact us and we will be happy to provide additional examples.

Chapter 7: Best Practices and Recommendations

Efficient cryptocurrency investigations frequently depend on cooperation between different parties, including:

- **Interagency collaboration:** By exchanging information and resources with other law enforcement organizations both locally and abroad, one can cast a broader net in order to capture criminals who take advantage of jurisdictions that span borders.
- Working with financial institutions and cryptocurrency exchanges can provide investigators access to specialist tools for tracking down and freezing illegal transactions.
- **Community involvement:** Establishing contacts with companies and bitcoin enthusiasts can help to promote confidence and the reporting of questionable activities.

Ongoing Education

Cryptocurrency is a dynamic industry. Fraud schemes develop regularly. Investigators must be set for a continuous journey of learning and training to have the upper hand on bad actors. Law enforcement must:

- **Monitor new trends actively:** It's essential to stay current on investment schemes, money laundering methods, and new cryptocurrency technology employed by criminals.

- **Invest in specialized training:** It's critical to arm investigators with the information and abilities necessary to examine blockchain transactions, identify suspicious wallets and understand how cryptocurrencies work.
- **Embrace:** Law enforcement must embrace specialized blockchain analytics and investigation tools and methods, to detect trending fraud and money laundering schemes.

The use of QLUE™ can greatly help investigators resolve cases swiftly. It uses public blockchain data to identify interconnections between wallet addresses, revealing suspicious links and identifying unlawful practices. It offers comprehensive analytics and visual representations of the flows of funds. Investigators can track and trace suspicious activity across different blockchains, and in many cases, quickly link them to entities.

Please reach out to us to set up a free trial of QLUE.

Step by Step Guide for Investigating Crypto Crimes

Step 1: Collect victim statements, screenshots, messaging conversations, and receipts.

- Look for crypto wallet addresses or transaction ID's
- Rely on the crypto amount that was transferred, not dollar amount. Due to price volatility, dollar values can fluctuate.
- Crypto ATMs charge high fees, which will affect the total amount sent
- Note that time stamps on receipts and screenshots may differ due to the difference between the transaction time, and the time that the transaction was actually recorded on the blockchain

Remember, it is critical to ensure that you have the correct starting point.

Having the correct starting point for your investigation is critical, as the information provided by the victim may be incomplete, or not accurately reflect what's recorded on the blockchain.

Step 2: Start your Investigation

Using information collected in step 1, ensure that you have the correct starting point. Begin your investigation and always consider the following:

- Confirm that the dates and times of transactions align with your victim's timeline.
- Use OSINT tools to try to identify any known wallets.
- How much value is still held in the addresses?
- Do the addresses have any exposure to entities (exchanges, payment processors)?
- When were the addresses last active?

Step 3: Know When to Stop Tracing

The goal when tracing is to follow your funds to an exchange, or known entity that collects KYC information. Knowing when to stop tracing will ensure that you don't go down the wrong path.

In general, you should stop tracing when you encounter:

- Exchanges or Crypto Businesses (VASPs) - this is the best case scenario
- Potential Service Addresses: These are addresses that have no direct attribution but have over 1,000 transactions, or are a part of a cluster (group) with over 500 other addresses. These are likely to be service addresses that have not been identified.
- Change of Address types: When following BTC forward, users need to be mindful of changes in Address types. This would indicate a possible payment made to a new wallet. There are 3 common address types you are most likely to encounter when investigating Bitcoin wallets:
  - Addresses that begin with 1: Referred to as Legacy or P2PKH.
  - Addresses that begin with 3: Referred to as pay-to-script-hash (P2SH), or script address.
  - Addresses that begin with bc1: Referred to as native SegWit or Bech32 addresses.
- Excessive comingling of funds: When the UTXO you are following is part of a transaction with multiple inputs and outputs it is advisable to stop investigating further. This is because you will not be able to link an input to a particular output.
- Avoid following Crypto through identified privacy services such as Mixers, Tumblers and Coinjoins.

If you're ever stuck, call us for help.

Step 4: Contacting an Exchange

Once funds flow to an exchange, investigators should stop tracing and proceed with contacting the VASP (Virtual Asset Service Provider),

Many crypto exchanges have a law enforcement portal or compliance liaison that you can contact directly. You can request the following information:

1. KYC information - Identifying information of account owner
2. Account Balance - Are the funds still in the account and recoverable
3. Trade history - Did they trade or swap the funds
4. Deposit/withdrawal history - Have other crypto funds been deposited or withdrawn
5. IP information - Where was this account accessed from

Step 5: Issuing Subpoenas

If the exchange does not have a law enforcement portal, or contact person, following jurisdiction-specific protocols, you can issue a subpoena.

- **Key Data Points to Subpoena**:
    a. Activity/IP address logs and multi-factor authentication logs
    b. Onboarding information and ID/selfie photos with verification reports
    c. Institutional documents (incorporation, ownership, business details)
    d. Transaction history (deposits, withdrawals, wallet addresses)
    e. Communication records (emails, phone calls, support tickets)

Step 6: What Next?

If your violators are local in the United States or within your jurisdiction, you can build a case and work toward enforcement action. This is generally done by working with a District Attorney.

Most often however, VASP records will indicate that there is an international connection. Cryptocurrency has enabled bad actors to move money across the globe from citizens in local jurisdictions at lightning speed, but it has also empowered local law enforcement to have international impact like has never been seen. Local law enforcement can use the KYC data obtained from VASPs to identify suspects and close cases. More importantly however, it has created the opportunity through voluntary compliant VASPs to seize stolen assets for return to victims, as well as seek forfeiture on large amounts of illicit proceeds.

If the violators are located outside of the United States, you may also opt to work with a US Attorney and a federal agency like the USSS or HSI to seize the funds. These agencies may or may not accept your case based on a variety of factors.

While it may feel discouraging, at the very least, you should be able to get information back to your victim to give them closure. It can be comforting to victims to hear that you know for certain where their money has gone and that, in some cases, it is highly unlikely that they will receive it back.

The other course of action is for the victim to pursue a civil lawsuit. Please reach out to us, and we can refer you to attorneys who specialize in pursuing crypto cases across international jurisdictions.

Get in Touch

BLOCKCHAIN INTELLIGENCE GROUP

Blockchain Intelligence Group (BIG) is a leading provider of blockchain analytics and compliance solutions. QLUE, our award-winning software platform's intuitive design, allows you to track and trace with confidence, even if you're new to cryptocurrency investigations.

Trusted by law enforcement agencies globally, our suite of products strips away the complexity of navigating through confusing blockchain data, providing visual transaction mapping and case file management. We provide powerful cryptocurrency investigation tools that fit any budget.

Contact us for a free trial of our investigative tools, if you would like some help with a case, or if you have any other questions.

sales@blockchaingroup.io - (844)-282-2140

The Block Audit

As fraud detectives, Jesse and Alex witnessed cryptocurrencies become criminals' preferred method for laundering stolen funds. Facing mounting caseloads and limited resources, they dedicated themselves to mastering crypto investigation techniques and understanding blockchain technology.

Founded in 2019, The Block Audit LLC was formed to empower local law enforcement to tackle cryptocurrency crime effectively. By providing investigators with practical knowledge and tools through free resources and contracted partnerships, they help protect victims and recover stolen assets.

info@theblockaudit.com - (954)-698-2700