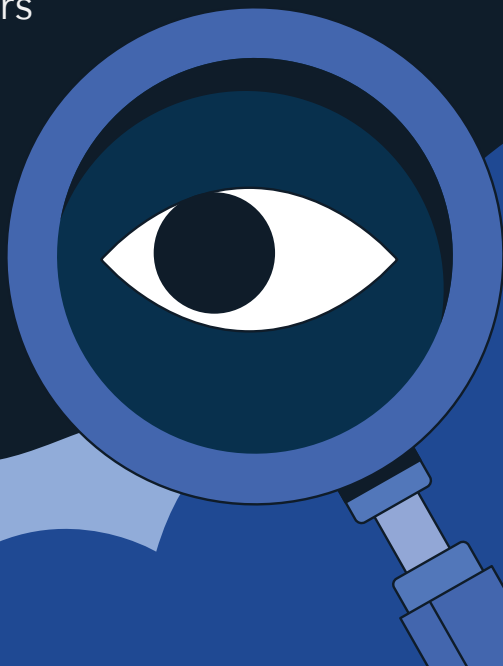




# Investigating Crypto Scams

A Flip Book for Law  
Enforcement Officers



TRMLABS.COM

TRM Labs' Crypto Scam Flipbook is an essential resource for investigators, police officers, and other law enforcement professionals who are encountering cryptocurrency scams and frauds. While many of the schemes may look familiar to those well-versed in traditional scams and hacks, the addition of blockchain technology presents new approaches for scammers and complexities for investigators. As the use of crypto in crime continues to rise, access to the right tools and education will allow all law enforcement personnel to identify common schemes, disrupt illicit activity, and assist victims in recovering funds.

This flipbook will outline key terminology, types of scams you may encounter, and the importance of blockchain intelligence to fight this illicit activity.

## About TRM Labs

As a leading blockchain intelligence company, TRM Labs helps institutions identify and investigate high risk cryptocurrency wallets, transactions, and entities.

The investigative goal of "blockchain tracing," generally, is to identify the actual controller of an otherwise pseudo-anonymous address. To do so, an investigator may be able to trace blockchain transactions and find counterparty exposure with an entity

or individual that can provide the identity of the beneficial controller of an address. More simply, an investigator should follow the money to or from an entity that can provide real-world identity.

While free and open source tools can be used to trace flows of potentially illicit funds, TRM's Graph Visualizer enriches blockchain data and models transactions in easy-to-build and understand graphs. These features allow the investigator to quickly identify exposure to entities that may be able to provide identification data in response to legal process submitted by a law enforcement officer.

TRM Labs also has numerous publications, tutorials, and expertise available for law enforcement, including a "duty investigator" assigned to manage the TRM Helpline 24 hours a day. Investigators, prosecutors, and other law enforcement professionals that need additional resources should contact TRM Labs for access to TRM Academy training & certifications, TRM LEO Labs, and TRM Training Days.

## Contact

Please reach out to [lerelations@trmlabs.com](mailto:lerelations@trmlabs.com) for additional information and resources for blockchain investigations.

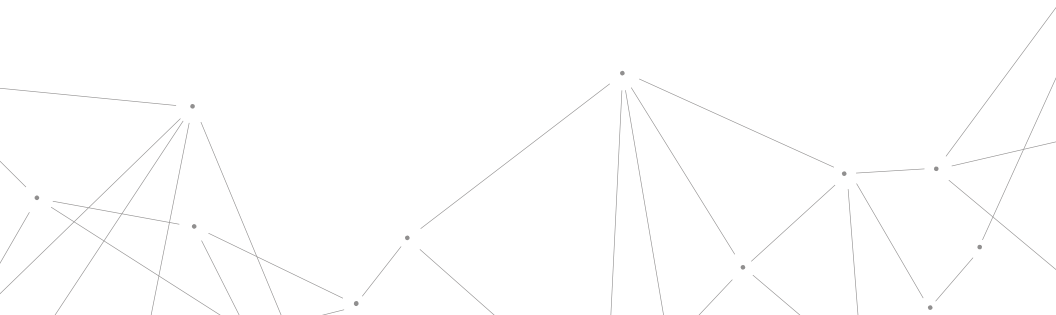
# Scam Types

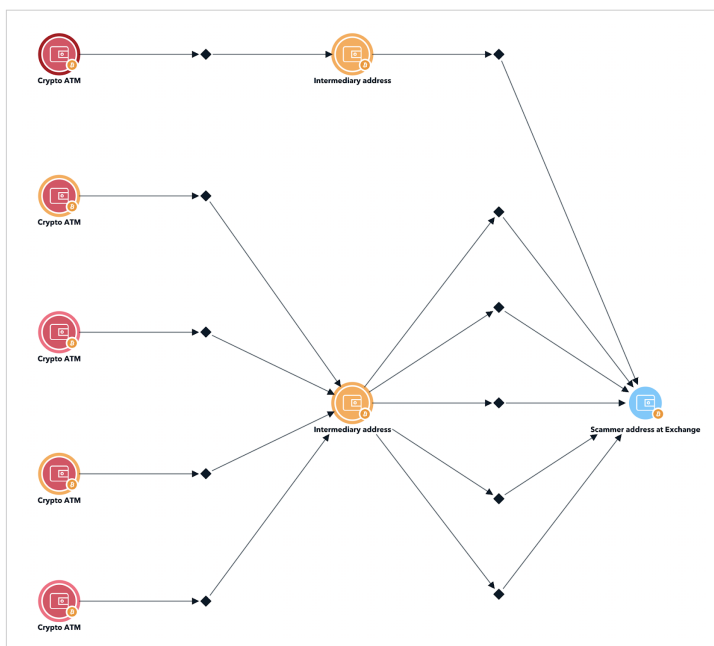
## Romance Scams

These scams occur when a fraudster adopts a fake online persona to gain a victim's affection and trust and uses the relationship to manipulate and/or steal from the victim. Many scammers first make contact on dating and social media sites, but quickly request victims communicate directly on encrypted communication platforms. Romance scammers make fraudulent promises of future romantic relationships and even marriage in order to induce the victim into providing the scammer with money, frequently in the form of virtual currency.

Romance scammers often claim to be located in remote locations with substandard internet in order to avoid engaging in face-to-face or video communication. This also offers the scammers a chance to deploy a common pretext for needing money from the victim: the scammer is either unable to access his/her bank account or needs money due to an emergent situation.

Typical on-chain activity for romance scams shows many incoming transactions, originating directly or indirectly from custodial VASPs or ATMs into aggregation addresses, which quickly cash out funds:





## Pig Butchering

A common type of scam, the term “pig butchering” is used to describe the process by which scammers “fatten up” their victims by obtaining increasingly more money from them prior to ending communication and stealing all their money. Also known by the phrase “Shā Zhū Pán,” in reference to their apparent origins in South East Asia, these crypto scams rely on psychological manipulation to induce victims to trust the scammers even when it seems unlikely that what the victim is being told is actually true.

A pig butchering scam occurs when a scammer builds a relationship with the victim over time and convinces the victim to invest in fraudulent or fictitious projects. The scammer tries to drain as much money out of the victim as possible, often using fake investment sites that advertise large false profits and/or social engineering techniques, such as intimidation via claims of owing taxes.

There are several common tactics that scammers use in these scams, including:

**Broker platform/investment scams:** Fake investment services cite incredible returns on investment, along with enormous savings, enticing potential customers. After the victim deposits money, the platform will show a large increase on their investment, encouraging the victim to deposit even more. Generally, the return-on-investment is fictitious. Once a victim attempts to withdraw funds he/she is unable to do so and the scammer generally ceases communications with the victim or asks them to pay more in order to complete the withdrawal.

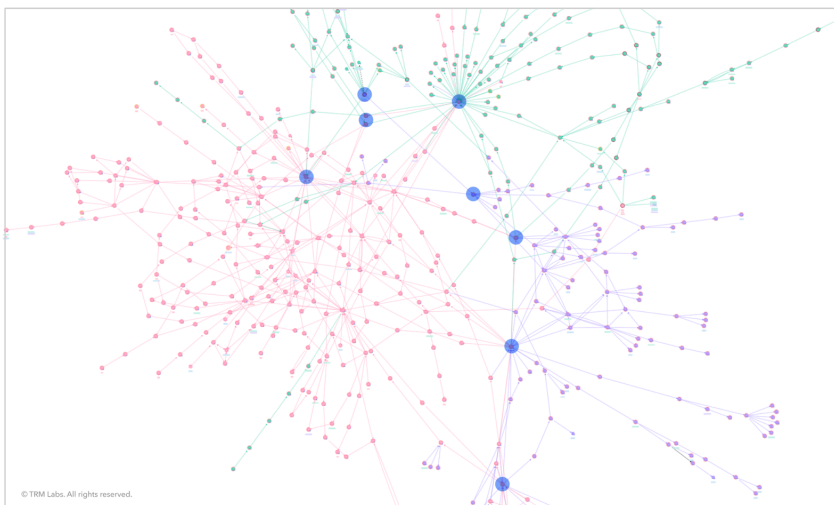
**Wrong number texts:** A scammer may send a "wrong number" or "accidental" message, either to a personal cell phone number or through a dating or social media app, which they use as a way to engage in a relationship with or befriend the victim. Once a relationship is cemented, the scammer will draw the victim's attention to false crypto investment opportunities or ask for monetary assistance for falsified personal struggles.

**Liquidity mining scams:** Liquidity mining refers to a process that incentivizes users to fund a liquidity pool, or crypto assets held by a smart contract that allow users to trade without relying on a centralized exchange, by rewarding them with additional tokens beyond the trading fees they earn. In Ethereum liquidity mining scams, illicit actors may take advantage of the complexity of the process to execute malicious code resulting in the misappropriation of the victim's funds.

**Government/authority extortion scams:** A scammer poses as a government official and contacts victims to inform them that there will be a negative consequence unless they pay a fee to the government entity in question. Generally, victims are groomed into paying all the liquid assets at their disposal in order to avoid arrest/fines/embarrassment.

On-chain, pig butchering proceeds often get converted into other currencies at decentralized exchanges. The funds typically enter what appear to be complicated money laundering networks that link multiple pig butchering schemes (see below image). Funds are sometimes swapped into currencies on other blockchains (often Tron) and/or converted into fiat currency via centralized exchanges, which is where law enforcement can often find the best leverage points.

Public reporting indicates that pig butchering schemes are likely conducted by professional criminal organizations, sometimes using human-trafficked persons to conduct the scams.



## Fictitious Projects and Fraudulent ICOs

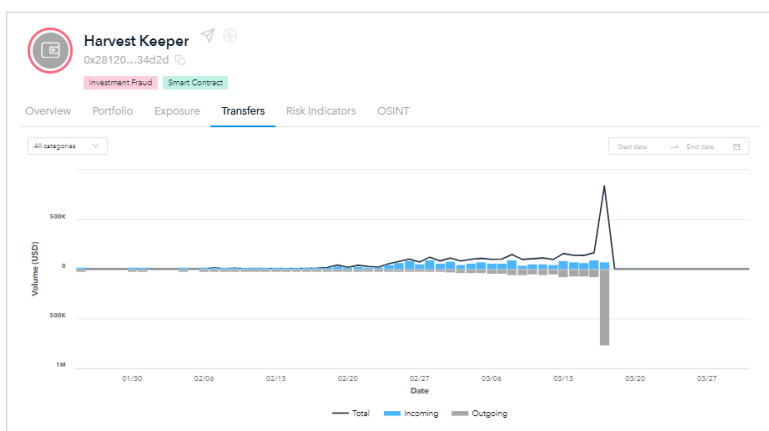
In this scenario, a scammer pretends to be building a project and solicits investments from victims. For example, scammers have created fake Initial Coin Offerings (ICOs) or fundraising events where new cryptocurrencies or tokens are offered to investors in exchange for established cryptocurrencies or fiat currency. Generally, the scammers have created real or perceived hype surrounding the launch using marketing and/or false representations to the public. Once the scammers have collected funds from victims, they often disappear. This is sometimes referred to as a “rug pull” or “exit scam.”

Generally, it is difficult to tell if a project is fraudulent based only on its blockchain footprint, at least at first, before it conducts an exit scam. However, sometimes signs of market manipulation can be identified, such as in wash trading of the relevant token to try to pump up its value. Investigators need to research the off-chain properties of the project to help determine its legitimacy, including any potential filing with regulatory authorities.

## Rug Pulls and Exit Scams

These are fraudulent schemes where the creators or developers of a crypto project intentionally abandon the project or manipulate its functionalities to steal investors' funds. Scammers typically deceive investors by initially presenting a seemingly legitimate and promising project and then abruptly exiting it with the funds invested by unsuspecting participants. Some rug pulls are complex investment vehicles while others are framed as exchanges, vendors on marketplaces, or unlicensed money service businesses.

Exit scams can happen slowly over time, though the creators of a project tend to withdraw as many funds as they can in one go. Their transfer activity over time often resembles the graphic below, where the large outgoing spike represents the exit scam. Funds are often pulled out of a smart contract or liquidity pool associated with the project.



## Pyramid and Ponzi Schemes

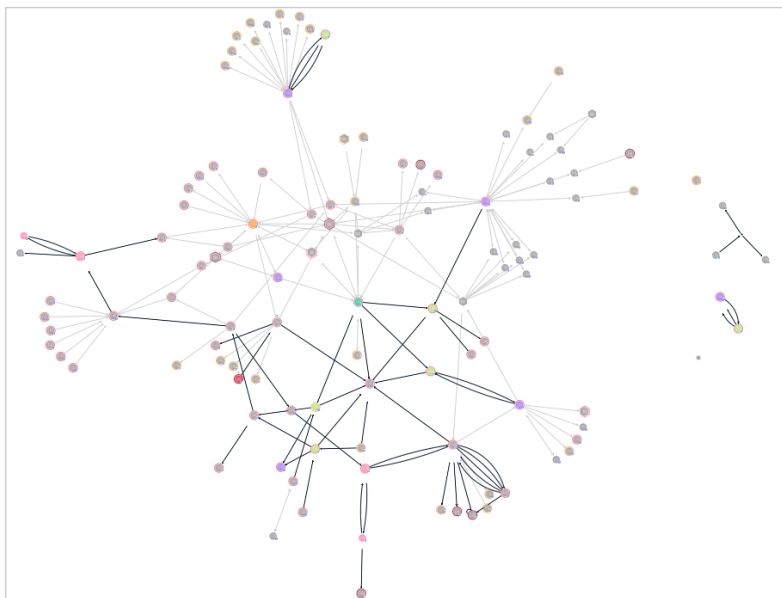
This type of investment scam promises high returns to investors, but the returns are actually paid from the funds of later investors, not from profits. As in traditional Ponzi schemes, these schemes may pay out the promised returns to the initial investors during the early stages in order to induce additional investment. To sustain the scheme, the operator focuses on recruiting new investors. They may employ various tactics, such as word-of-mouth referrals, social media marketing, or hosting seminars and events to target potential victims. The promise of high returns and the success stories of early investors are used to entice new participants. Many schemes also have strong pyramid-scheme-like elements where the users themselves get strong incentives for recruiting as many people as possible.

Instead of investing the funds in legitimate ventures as promised, the operator diverts the majority of the incoming investments for personal use or to pay off earlier investors. Only a small portion of the funds may be used for actual investments or operations to maintain the illusion of a legitimate business. As the scheme relies solely on recruiting new investors to sustain itself, it does not generate legitimate revenue from investments or productive activities. The flow of new funds is essential to meet the withdrawal requests of existing investors and to maintain the appearance of a successful venture. Once new investment slows down or hits a saturation point, the scheme collapses and most investors are left with significant losses.

Ponzi and pyramid schemes generally have the most complicated on-chain activity of all the other scams mentioned. Because fraudsters make payouts to investors, it can be hard to determine what might be a withdrawal to an investor vs. a withdrawal to the scheme operator. Additionally, fraudsters often use third party payment processors to accept deposits and make withdrawals to users, which complicates the on-chain investigation and sometimes necessitates legal process to identify what activity of the payment processor is related to the scheme.

The schemes can have some simple activity, but they often have multiple aggregation, intermediary, and withdrawal addresses. Sometimes they have one deposit address per user, while other times they share deposit addresses between users or create new ones for every deposit.

The below image shows a partial tracing of the deposit and withdrawal infrastructure of the Finiko Ponzi scheme, which sometimes utilized a payment processor for its operations.





In this type of scam, the victim is persuaded to pay a sum of money upfront in the promise of receiving a larger amount of money at a later date. In a crypto version of this scam, a scammer might promise a large quantity of cryptocurrency in return for a smaller upfront payment.

[illegible]

In these schemes, scammers will heavily promote a particular cryptocurrency to inflate its price (the "pump"). Once the price has risen significantly, they sell off their holdings in that currency, causing the price to crash (the "dump"). The scammers profit, while those who bought in during the "pump" phase lose money. In many pump-and-dump schemes, the scammer misrepresents the total assets associated with the scheme and/or the scammers beneficial interest in the assets.

Global search results

- Amazon\_Pump\_Signal\_Coinbase**  
@Amazon\_Pump\_Signal\_Coinbase
- FL Crypto Pumps**   
@F\_crypto\_pumps\_I
- Crypto Pump**  
@pump
- Kucoin Binance Pumps Trading**  
@Kucoin\_Binance\_Pumps
- Pumps Signals Trading Whales**  
@Pumps\_Signals\_Trading\_Whales
- Btc Bitcoin Signals Pumps**  
@Btc\_Bitcoin\_Pumps\_Signals
- Coinbase Signals Pumps**  
@Coinbase\_Signals\_Pumps
- Dogecoin Pumps Signals**  
@Dogecoin\_Pumps\_Signals

**Pumps Signals Trading Whales**  
754,228 subscribers

**Pinned message**  
Reached a peak of 431% after our signal, making a...

Get our signals before everyone else.  
Don't miss out the chance to take part in our successful story of changing the financial life of so many.

We are also doing a private event exclusively for our VIP Members this week.  
Only 3 slots left! 🔥🔥🔥

If you want to join and buy our VIP Membership please fill our google form or try our Automated Bot system!

@Kucoin\_Binance\_Pumps\_Bot

<https://forms.gle/knnrHtFA54qEp3f6>

[Google Docs](#)  
**KUCOIN BINANCE PUMP VIP GROUP**  
VIP: Valid for 72hours!  
LIFETIME VIP MEMBERSHIP PRICE:  
250 USDT (DISCOUNT PRICE)...

456.6K 8:00 AM

[JOIN CHANNEL](#)

On-chain, you generally see evidence of a lot of trading of the token being pumped, while on price-watching applications available at many exchanges and other services, you might see the price spike suddenly before either gradually or suddenly falling.



## Phishing Scams

Scammers will impersonate a reputable cryptocurrency service (like a wallet or exchange) and send victims emails, text messages, social media messages, or even cryptocurrency tokens with a link to a fraudulent website. Sometimes scammers will even create fake Google ads hoping that when an individual searches for the legitimate site, they'll accidentally click on the link in the search results to the phishing site instead. The aim is to trick the victim into entering their login credentials or seed phrase, which the scammer then uses to access the victim's account and steal their funds.

## NFT Bait-and-Switch Phishing Scams

This form of phishing prompts users to sign a contract, usually under the pretense of a legitimate transfer of ownership, which then grants control of the user's entire wallet to the attacker.

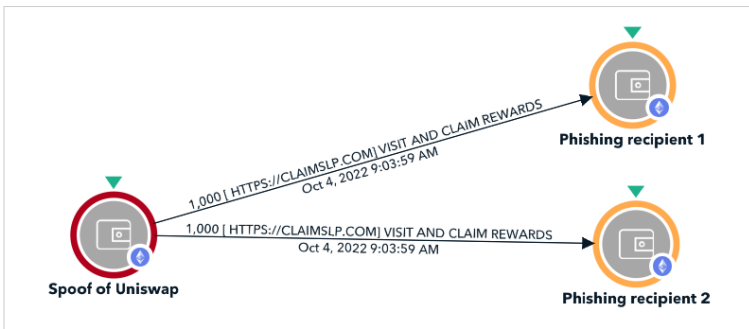
A step-by-step look at how it typically works:

1. The attacker sets up a wallet.
2. The attacker creates a contract. The bait-and-switch contract includes code functions that may allow an attacker to transfer all of the victim's tokens from the victim's wallet.
3. The attacker deploys a contract initiating the transfer.
4. The attacker phishes the victim. The actual phishing can take different forms, including emails, DMs in messaging apps, pop-ups on forums, in-wallet ads, fake sites with wallet connections, impersonations of support staff on NFT markets. In the end, the victim is always asked to either provide private keys or sign approval contracts. These attacks are successful because buyers and sellers are under pressure to act fast to collect valuable NFTs.
5. The attacker steals the NFT.

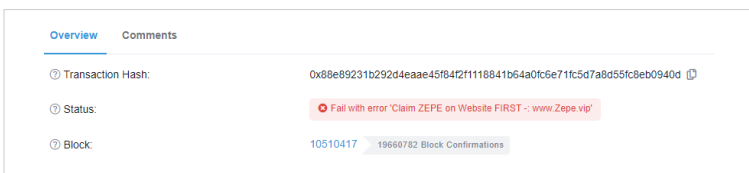
## Airdrop Phishing

One common form of phishing involves airdropping tokens to users' wallets with the goal of getting the users to research the token and end up on a website controlled by the scammer that will steal the user's login information or allow an approval to let the scammer remove funds from the user's wallet.

In the below example, the token name is the phishing website name. The scammer sent the tokens to thousands of users and also spoofed UniSwap to make it look like UniSwap was the one airdropping the tokens when in fact they did not.



In another form, the scammer might purposefully do the airdrop wrong to get the user to visit a block explorer, where the user might see something like the below image, which could prompt them to visit the website.



## Drainware

Drainware is a smart contract code written in a way that enables attackers to sweep NFTs or crypto directly from users wallets. The draining occurs when a user unknowingly connects and signs a transaction attempting to either purchase and mint an NFT, or through interaction with a phishing website that is imitating a legitimate crypto service. Drainware contracts are considered malicious because they are specifically designed with the purpose of theft and have no other legitimate uses. Drainer Templates as a Service (DTaaS) have also surfaced, providing attackers pre-built, ready-to-launch drainware templates.

## Mining Scams

These scams promise victims high returns from participating in cryptocurrency mining, often asking for an upfront payment for "shares" in a mining pool. However, the mining pool either does not exist, it does not pay out the returns that were promised, and/or it turns out to be a Ponzi/pyramid scheme (as in the below example).

A popular form of the mining scam is "USDT Mining" scams, which tells users they're mining USDT, usually on Tron, which is not actually possible. As mentioned above, "liquidity mining" was also a popular term used by pig butchering schemes in the past, though it appears less common currently.

**Please select your plan**

Swipe investing ideas into action with a full range of investments.  
Enjoy real benefits and rewards on your accrue investing.

FREE-BLOCK	LITE-BLOCK	MINI-BLOCK	MEGA-BLOCK	ADVANCED-BLOCK <small>BEST OFFER</small>
0.10 USDT.TRC20	15.00 USDT.TRC20	30.00 USDT.TRC20	60.00 USDT.TRC20	100.00 USDT.TRC20
Earning rate: ₹ 0.03000000 per day	Earning rate: ₹ 7.50000000 per day	Earning rate: ₹ 16.50000000 per day	Earning rate: ₹ 36.00000000 per day	Earning rate: ₹ 85.00000000 per day
Affiliate Bonus: 5.00% Duration: 365 days	Affiliate Bonus: 40.00% Duration: 4 days	Affiliate Bonus: 40.00% Duration: 4 days	Affiliate Bonus: 50.00% Duration: 4 days	Affiliate Bonus: 55.00% Duration: 2 days
<a href="#">LOGIN TO BUY</a>	<a href="#">LOGIN TO BUY</a>	<a href="#">LOGIN TO BUY</a>	<a href="#">LOGIN TO BUY</a>	<a href="#">LOGIN TO BUY</a>

These mining schemes usually end up at least attempting to be pyramid schemes and so have on-chain patterns consistent with that of pyramid and Ponzi schemes.

## Tech and IT Support Scams

Fraudulent activities where scammers pose as technical support personnel or representatives of cryptocurrency platforms to deceive victims and steal their funds or sensitive information. These scams typically involve exploiting the victims' lack of technical knowledge or familiarity with cryptocurrencies.

Typically the process goes like this:

**Initial Contact:** Scammers reach out to potential victims through various channels, such as phone calls, emails, or online advertisements. They may claim to be from a reputable cryptocurrency exchange, wallet provider, or technical support company associated with cryptocurrencies. Or they may claim to be from a company completely unrelated to crypto, such as Microsoft or Geek Squad.

**Creating a Sense of Urgency:** Scammers often employ tactics to create a sense of urgency or fear in their victims. They might claim that the victim's cryptocurrency wallet or account has been compromised, there is suspicious activity, or there is an urgent need to update security settings.

**Gaining Remote Access:** To gain the victim's trust, scammers may request remote access to the victim's computer or mobile device. They use various methods, such as directing victims to install remote access software or manipulating victims into providing access to their devices through phishing techniques.

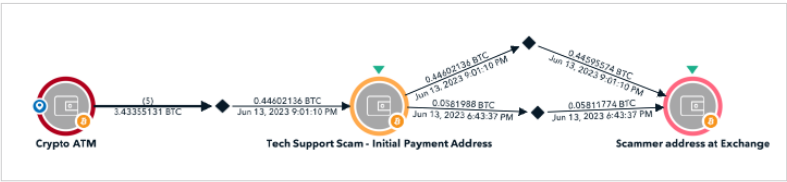
**False Technical Support:** Once the scammer gains remote access, they pretend to diagnose and fix alleged technical issues. They might show the victim fake error messages or claim to perform actions to resolve the problems, all while appearing helpful and professional.

**Requesting Payment or Personal Information:** As part of the scam, scammers may request payment for their services or claim that certain fees need to be paid to resolve the issue. They might ask victims to provide credit card information, cryptocurrency wallet details, or other sensitive personal information under the guise of resolving the technical problem. Sometimes they even create the customer's crypto account for them while remote accessing their computer.

**Theft or Further Exploitation:** If the victim complies with the scammers' requests, they may steal funds from the victim's cryptocurrency wallet or gain access to their personal accounts, leading to financial loss. Additionally, scammers may use the obtained personal information for identity theft or further fraudulent activities.

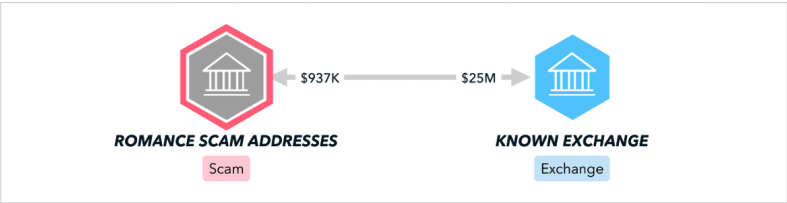
The on-chain activity of these tends to be relatively simple as well. The below image shows an example of the victim sending funds to the scammer’s address via ATM before the scammer then sends it directly to an exchange.

Other times though, the scammer might, for example, send the proceeds directly through a mixer to attempt to obfuscate the source of funds.



## Impersonation Scams

Scammers may impersonate a government agency, such as a tax authority or law enforcement agency, and threaten the victim with claims such as: “you owe taxes, send us money or you will be arrested.” Or, in family emergency scams, suspects impersonate a family member who they claim to be hurt or in trouble with the police and need money, in the form of crypto, to help them.



## Extortion Scams

Similar to impersonating the government, in extortion scams, scammers will claim something bad will happen to the victim if he or she does not send the extortionist crypto. The bad event could be exposing personal, family, or business information, threat of government action or inaction, threats of cyber intrusions, or even threats of physical violence.

A common version is the “sextortion” scam, where scammers will send users messages saying they have hacked their computer, accessed their webcam, and obtained compromising video of the victim before demanding payment for not releasing the footage.

chainabuse

Report a Scam

Top

Reports submitted for

1 Scam Reports

Other Blackmail Scam

Threatening to make all my data public as well as release a video supposedly featuring my face from a webcam and pornography. Offered no evidence to this claim and I have seen this message copy and pasted to Reddit sent from other addresses to people on Reddit.

Submitted in Bitcoinabuse on Feb 19, 2022

Reported Address

## Inheritance and Lottery Scams

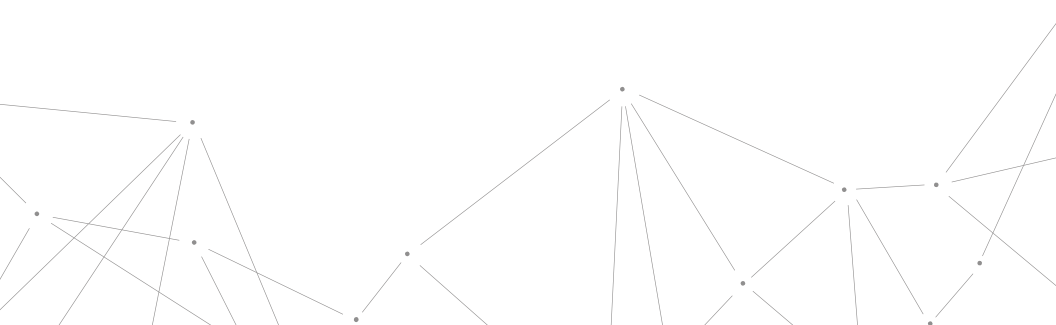
Usually a type of advance fee fraud, in inheritance scams, criminals often initiate contact via email, social media, or even traditional mail, claiming to be lawyers, representatives of deceased individuals, or family members. In lottery scams, criminals set up websites or send emails claiming that the recipient has won a significant amount of cryptocurrency in a lottery or giveaway.

In both cases, they inform the target that they are the rightful heir or beneficiary of a substantial amount of cryptocurrency left behind by a deceased person or won in a lottery. The scammers will often ask the victim for funds on several different occasions to “unlock” the full amount.

## Money Mule Scams

Scammers recruit individuals, known as money mules, to facilitate the transfer of illicit funds obtained through illegal activities. In the context of cryptocurrencies, money mules are used to move and launder money earned through various fraudulent activities, such as phishing, hacking, or cryptocurrency investment scams. The money mules may be asked to send some of their own funds as well. In the context of a money mule scam, mules do not know they are conducting illicit activity.

Criminals will generally try to send their illicitly earned crypto to mules at exchanges or peer-to-peer services to have them move funds on their behalf.



# Using blockchain intelligence to investigate cryptocurrency-based scams

There are many paths to success in disrupting cryptocurrency-based fraud schemes. Though frauds can vary significantly as can the laundering techniques used to conceal the source and destination of the fraudulent proceeds, blockchain investigators should have two primary goals in mind when opening a cryptocurrency-based fraud investigation: (a) identify the fraudsters, and (b) freeze, seize and return victim funds.

To do so, TRM recommends these general, broad steps for identifying the fraudster and forfeiting the misappropriated funds:


1. Identify transactions associated with scam.
  2. Trace proceeds of scam on blockchain.
  3. Identify and request records from any third party with exposure to the fraudster or its proceeds.
  4. Request Legal Process and Production of Records from third party.
  5. Freeze and/or seize all assets associated with the scam.
  6. Identify and charge scammers with violations of criminal law.

## 1. Identify transactions associated with scam

Details of a scam may come to law enforcement in many ways. An investigator may take a victim complaint, read a report from a crowd-sourced scam website like chainabuse.com, or read about a scam in a SAR. Many fraudsters `cash-out` proceeds from the fraud schemes within 24 hours, so time is of the essence for a blockchain investigator.

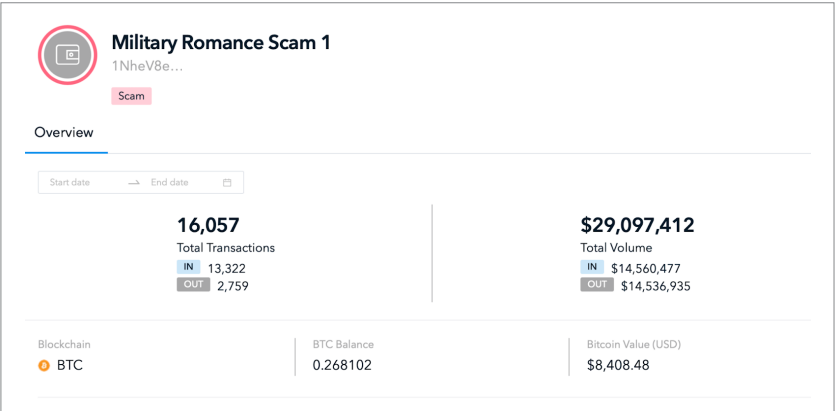
The investigator should therefore attempt to quickly verify the reported loss amount, determine if stolen assets are still in the cryptocurrency ecosystem, and attempt to ascertain whether there is a third party that can be contacted to learn the disposition of funds and/or the identity of the fraudsters.

To do so, an investigator should seek to identify virtual currency addresses and transaction IDs within the complaint. For example, the blockchain investigator may look for the following types of alphanumeric sequences, QR codes, and transaction IDs in order to quickly learn about the addresses involved in a scam:

What it is	What it looks like
Bitcoin Address	1NheV8eQfHuVHLd25ggoMy5dbUBLVUygGz
Bitcoin Private Key	Kz7R5J9inisbtaNDz6cE439WAiycvkJ96Y1GZvqv8SgSQNPb4ZN5
Ethereum Address	0x522Dc35101654B48f31f494613E8A5155A371E68
Ethereum Private Key	184e9386f1d2587ebf1645ef1bf83df19a25080a7501a76b0acced158fed8e7
Transaction Hash	6146ccf6a66d994f7c363db875e31ca35581450a4bf6d3be6cc9ac79233a69d0
Bitcoin Address QR Code	<div></div> <div>1NheV8eQfHuVHLd25ggoMy5dbUBLVUygGz</div>

After identifying the addresses and/or transaction hashes, an investigator can input the information into blockchain intelligence tools such as ‘TRM Tactical’ or ‘TRM Forensics’ to learn about the transactions.

For example, after inputting an address into ‘TRM Forensics,’ an investigator could return results similar to the below:



As can be seen in the figure above, the blockchain investigator would see that the addresses is labeled as a scam (“Military Romance Scam 1”), there is substantial volume into and out of the address (\$29,097,412), the current balance of the address (.27 BTC or \$8,408), and where an address has direct or indirect exposure to a third party.

2. Using blockchain tracing to follow proceeds of scam

After obtaining a snapshot of the alleged scam from a blockchain intelligence tool, the investigator can quickly begin tracing proceeds forward and backwards from the fraudulent transaction(s). Doing so will enable the investigator to potentially identify ‘cash-out’ points and the presence of the other victims.

As seen in the TRM Forensics figure below, where Victim 1 informs the investigator that he sent funds to the “Scammer Address,” the blockchain investigator should:

**A)** Copy/paste receiving address (“Scammer Address”) into blockchain intelligence software.

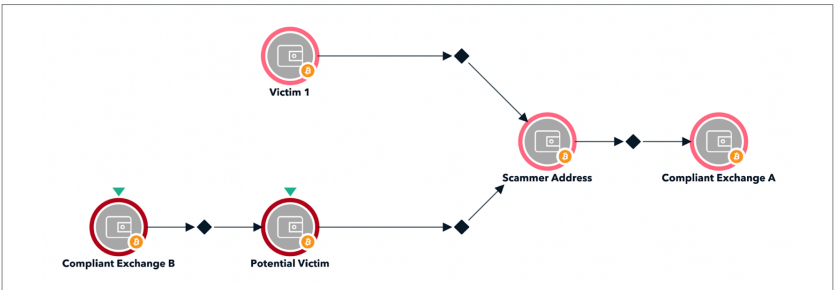
**B)** Identify subsequent addresses which received funds from “Scammer Address,” in this case, “Compliant Exchange A.”

[Once the investigator traces funds from the Victim, to “Scammer Address” and then to “Compliant Exchange A,” she should request “Compliant Exchange A” to freeze the funds and produce records associated with the controller of the address. More on working with exchanges in Step 3].

**C)** The blockchain investigator should then “trace backwards” from the “Scammer Address” in order to identify additional potential victims, in this situation, “Potential Victim” address.

(i) There is considerable likelihood that any additional incoming funds to “Scammer Address” are also proceeds of fraud.

**D)** In order to identify the controller of the “Potential Victim” address, the investigator should trace backwards to the origination of the funds; in this situation “Compliant Exchange B.” “Compliant Exchange B” may be able to provide records that reveal the identity of the individual controlling “Potential Victim” address.





In addition to blockchain intelligence software like 'TRM Labs' Graph Visualizer,' there are also public blockchain intelligence tools which allow investigators to manually track the flow of funds and allow users to analyze information on the blockchain. They often provide data such as:

**Transaction Information:** Search for specific transactions by entering the transaction hash or address. The tools display detailed information about the transaction, including the sending and recipient addresses, transaction amount, timestamp, and transaction status.

**Address Information:** Enter a specific address into the explorer to view transactions associated with that address.

**Block Information:** Explore individual blocks within the blockchain. Each block contains a set of transactions, and the explorer provides information such as the block height, timestamp, size, and the list of transactions included in that block.

**Network Statistics:** View real-time statistics about the blockchain network, including the total number of blocks, transactions per second, network hash rate, and other relevant metrics. This helps users gauge the network's health and activity.

**Token and Contract Information:** Better understand different tokens, including their supply, token holders, contract details, and which address created the smart contract or token.

**Visualization:** Some explorers offer visual representations of the blockchain data, such as graphs or charts, to help users understand the network's structure, transaction volume, or address interactions. These visualizations can aid in identifying patterns, trends, or anomalies within the blockchain.

**Advanced Search and Filtering:** Narrow down queries and find specific transactions, addresses, or blocks based on various parameters like time range, transaction type, or block height.

One free, open-source blockchain explorer called Etherscan.io enables users to view every transaction ever conducted on the Ethereum blockchain. It shows up-to-date transactions between addresses in real-time and offers additional information about smart contracts and data associated with assets which use the Ethereum blockchain:

Etherscan

Home

Blockchain

Tokens

NFTs

Resources

Developers

More

Sign In

Transactions

For Block 17693621

Sponsored: 

METAWIN

. The First Web3 Casino. Instant Payments, Instant Play. No Registration Required. [Play NOW](#)

A total of 136 transactions found

First

Page 1 of 3

Last

<div>⌵</div> <div>Txn Hash</div>	<div>⌵</div> <div>Method</div>	Block	Age	From	To	Value	Txn Fee
<div>⌵</div> <div>0x5f7278c4e1b0aaff73...</div>	<div>Transfer</div>	17693621	27 secs ago	<a href="#">beaverbuild</a>	<div>⌵</div> <div>Lido: Execution Layer R...</div>	0.052004159 ETH	0.00052423
<div>⌵</div> <div>0xdad383a78bd0c06a...</div>	<div>Transfer</div>	17693621	27 secs ago	<div>0x8c807C...564d7465</div>	<div>⌵</div> <div>0xc1e405...7f356742</div>	0.032830161 ETH	0.0004981
<div>⌵</div> <div>0x9c925ebda3e573660...</div>	<div>Transfer</div>	17693621	27 secs ago	<div>0x84a576...3A125a12</div>	<div>⌵</div> <div>0xK5C97A...b333e499</div>	0.012 ETH	0.0004981
<div>⌵</div> <div>0xd7046aa844a3ec4f...</div>	<div>Transfer</div>	17693621	27 secs ago	<div>0x5a593D...DA9C861</div>	<div>⌵</div> <div>0xK5F0c7...1368E205</div>	0.05 ETH	0.0004981
<div>⌵</div> <div>0xf1347780b29a10cd...</div>	<div>Transfer*</div>	17693621	27 secs ago	<div>0x5050F6...5867c49</div>	<div>⌵</div> <div>0xKFD000...0000a843</div>	0 ETH	0.00138139
<div>⌵</div> <div>0x428ac542935955e1...</div>	<div>Add Sequenc...</div>	17693621	27 secs ago	<div>Arbitrum: Batch Submitt...</div>	<div>⌵</div> <div>Arbitrum: Sequencer Inb...</div>	0 ETH	0.04365149
<div>⌵</div> <div>0x38548d6de3abdc6f98...</div>	<div>Uniswap</div>	17693621	27 secs ago	<div>0xcdaD46...9249727F</div>	<div>⌵</div> <div>1inch v5: Aggregation R...</div>	0.3 ETH	0.00345371
<div>⌵</div> <div>0xf01021216a208423cc...</div>	<div>Swap</div>	17693621	27 secs ago	<div>0x76658B3...Ca30F806</div>	<div>⌵</div> <div>1inch v5: Aggregation R...</div>	0 ETH	0.00413216

## TRM Forensics

While free and open source tools can be used to manually trace flows of potentially illicit funds, blockchain intelligence tools such as 'TRM Forensics' provide enriched blockchain data which includes attribution, open source intelligence, pattern recognition, visualization functions, and other features to help accelerate investigations. TRM Forensics includes enriched data related to 28 different blockchains, thousands of different virtual currencies, and millions of addresses - all with a graphical user interface.

These features allow the investigator to quickly follow funds from inception to disposition and may offer the investigator the opportunity to quickly identify the scammer and/or freeze and seize stolen assets.

### 3. Identify and request records from any third party associated with the scam or proceeds from the scam

Once an investigator traces funds to and from the scammer's address, the investigator will hopefully find “exposure” to an entity that collects and holds records and assets associated with the scammer. As detailed in Step 2, the investigator hopes to find the origination and disposition of funds associated with victims and fraudsters.

Frequently, both victims and scammers use third-party Virtual Asset Service Providers (VASPs) to convert traditional fiat currency to virtual currency and virtual currency to fiat currency. Many VASPs collect and maintain a cache of “Know Your Customer” information, many perform asset custody for customers, and many will work with law enforcement to provide records and perform freezes and seizures of illicit funds.

Almost every cryptocurrency-based fraud scheme involves the fraudster sending the proceeds of the scheme to a third party VASP. Identifying and working with third parties is the key to disrupting the schemes.

### 4. Legal process requests and production

Most third parties and VASPs will work with law enforcement, regardless of location of the third party and jurisdiction of law enforcement, provided the law enforcement request is legitimate and the third party's preferred process is followed. Foreign VASPs will frequently work with local, state, and federal law enforcement, even if not compelled to do so by law or treaty.

One way to quickly identify how to and where to serve process is to use a blockchain investigation tool such as TRM Labs ‘Know Your VASP’ which includes information such as location, contact information, KYC availability, and financial profile:

▼ About

Description

Coinbase is a U.S.-based cryptocurrency exchange that offers an array of blockchain-related services. Coinbase is building the crypto economy - a more fair, accessible, efficient, and transparent financial system for the internet age that leverages crypto assets: digital assets built using blockchain technology.

Headquarters

San Francisco, CA, USA

▼ Law Enforcement Contact

Law enforcement contact

For law enforcement officers, legal process/information requests for criminal matters should be directed to the Coinbase LE Portal:  
<https://app.kodex.us/coinbase/signup>

Follow the link above to begin your registration process and submit your request. You will be able to receive the records through the portal and keep track of your cases. If you have an exigent request, please make sure to mark your case "Exigent" under case type and we will process it right away.

Please note the portal only works in Google Chrome and Microsoft Edge.

For further questions, email Coinbase at:

KYC Details

KYC Level 3

ID verification and ID upload required during signup process.

During account creation:

• Full name

• Email

• State

• SMS authentication

During identity verification (during account creation process):

• Full Name

• Date of Birth

• Address

• Type of activity

• Source of funds

• Employment status

• Last 4 digits of SSN

• ID Upload

• Passport or Driver License (US), Government-issued ID, National ID Card, or Passport (Outside of US)

KYC Level

Level 3: The entity requires personal information and uploaded proof that the information is correct in order to withdraw/transfer crypto

What to provide to the third party when making a request:

User information:

When requesting information about a specific user or account, such as the victim or fraudster, an investigator should provide any available details about the account holder, such as the virtual currency address, an account's username, email address, or any other identifiers associated with the account.

Transaction information:

Transaction IDs, wallet addresses involved (including deposit, or receiving, addresses at the VASP), dates and times of transactions, and any other relevant information that helps the exchange locate the desired transaction records.

The image below from TRM's ‘Graph Visualizer’ displays key pieces of data such as the deposit address, transaction hash, and transaction timestamp.

The diagram illustrates a Bitcoin transaction on a blockchain. It shows a flow from a source address, **1H58wV...qQvo** (labeled as Romance Scam Addresses), to a destination address, **1554GU...pLHW** (labeled as Known Exchange Address). The transaction is identified by the hash **ed545e5ec49ae62c6e74a9f332b8178189825085839580110013f252ba68ab82** and occurred on **Jun 7, 2023 7:23:27 AM**. The transaction amount is **0.14907729 BTC**. A large blue arrow points from the transaction details to the transaction hash and timestamp.

If the investigator were interested in seizing the assets associated with the transaction above, or learning the identity of the controller of the address, the investigator would ask for all records associated with address “1554GU...pLHW” which received .14907729 BTC on June 7, 2023 via transaction “ed545e5ec...”

17\_ INVESTIGATING SCAMS USING BLOCKCHAIN INTEL

Depending on the level of KYC of an entity, as well as the robustness of their compliance program, it may be possible to request and receive the following information on your requested account(s):

- Government issued identification.
- Subscriber information, such as: account holder name, address, DOB, country, picture, email address, IP address.
- Associated accounts, such as linked credit cards or bank accounts.
- Account balances.
- Internal and external transactional history.
- Transactional counterparties.
- Communications and messaging.
- User device IDs.
- An omnibus “all records associated with the account and registrant.”

**NOTE:** Keep in mind that while the controller of the account may be the main subject, the named account holder could be a straw identity, a money mule, a stolen identity, or a professional money launderer.

## 5. Seize all assets (and/or facilities) associated with the scam

The most important thing to note here is that virtual assets CAN be seized. Where there are virtual currency assets involved in the effectuation of a crime, an investigator should endeavor to seize and restrain those assets (also known as pursuing confiscation in many regions). The multi-pronged purpose of asset confiscation is to punish criminal behavior, return assets to victims, deter illegal activity, remove tools that facilitate illegal behavior, disrupt criminal organizations, and protect the community.

Seizing crypto assets comes down to identifying who is in control of the private key that allows for transfer of the funds. Whoever controls the keys controls the asset.

### Victim funds held at a VASP

In situations where the funds are in possession of an identified VASP, the seizure must be made from the VASP. Many VASPs will not only accept legal process and judicial documents such as seizure warrants, many will accept unofficial “request to freeze” from law enforcement. Certain VASPs can be contacted by “click-of-a-button” within TRM’s ‘Forensics’ to alert the VASP of an emergent situation or request to freeze.

The best practice for an investigator is to immediately contact the VASP where victim funds are held, explain the situation, and request the VASP flag or freeze the transaction. Subsequently, the investigator should diligently work with partners to obtain judicial documentation of the request to freeze or seize the funds.

Finally, many VASPs have highly skilled Investigations units in addition to compliance units. Where an investigator may not be able to understand the full scope or complex nature of a scam, the investigator may want to consider contacting the Investigations team at the VASP for help. TRM Labs can usually provide a point-of-contact for an investigations team at most VASPs.

Once an investigator has authority to seize assets from a VASP, the investigator needs to move the assets into a government controlled wallet.

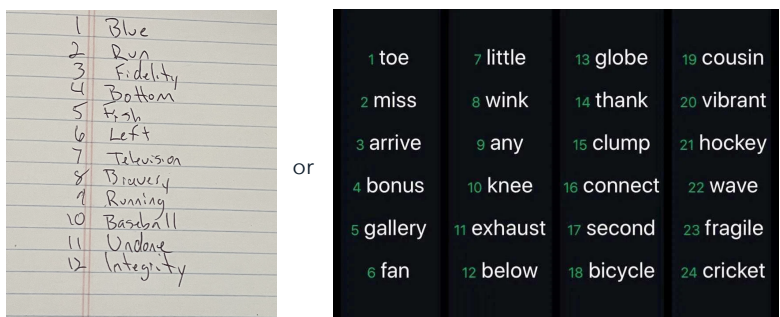
### Victim funds held in unhosted address

In situations where the fraudster is in control of the private key(s), such as funds being stored in a fraudster's unhosted wallet on his phone/laptop, the unhosted wallet's private key will need to be entered in order to move the funds to a government controlled account.

Depending on jurisdiction, there may be very little a government entity can do to compel someone to supply the private key, other than threat of punishment for defying a court order. Therefore, an investigator should consider convincing the controller of the private keys to provide the private key to the government by either positive or negative reinforcement.

Should that not work, the investigator should consider searching both electronic and hard copy facilities owned by the controller of the private keys. The investigator should search for both alphanumeric phrases and English word “seed phrases,” which can be backup private keys. “Seed Phrases” are generally 12-24 English language words, sequenced in order, which can be inputted into wallet software to reconstitute a cryptocurrency wallet and send funds.

A typical seed phrase may look like:



**How the government should custody seized assets**

Once an investigator has authority to seize assets, the investigator needs to move the assets into a government controlled wallet.

Procedures and opinions differ across jurisdictions and agencies for how to custody seized assets. What is universal, however, is that once a government “seizes” a cryptocurrency asset, it must move that asset into a government controlled or created wallet. An investigator must not rely on seizing a cell phone, application, or access to an account to effectuate a seizure. As discussed, if anyone else retains the private key to a physically seized wallet, that person can reconstitute a wallet elsewhere and move the funds, even where a subject may be incarcerated and the subject’s physical wallet confiscated.

Some law enforcement entities use hardware wallets for seizure, some use electronic wallets, some open accounts at exchanges, and some use combinations of these strategies. Whichever method is pursued, some considerations to make, prior to any seizure:

- Who will have access to the private keys of the government wallet (the investigator, the supervisor, in-house forfeiture staff, legal counsel, prosecutor)?
- Where will the hardware wallet/privatekey/access to the account be stored and who will have access?
- How will the government eventually return the asset to the victims or claimants (liquidated into USD, same form as seized)?
- If the asset will be liquidated, how will the forfeiture/liquidation be effectuated?

**6. Charging scammers with crimes**

Many cryptocurrency-based scams are multi-jurisdictional or international. This makes the charging process onerous and potentially unfruitful, as many jurisdictions are unwilling or unable to prioritize extraditions of scammers. However, there are many reasons for pursuing charges against scammers even where there may not be a guarantee of incarceration.

**Name and shame**

Most compliant and professional VASPs employ robust compliance staff and follow strict compliance protocols. Part of on-boarding new customers generally involves a due diligence check where a compliance staff may check open source records for negative information. Where there is a public charge for running a scam, a professional VASP will not allow a charged scammer to open an account, making future scams more difficult to monetize.

**International cooperation**

Due to its borderless nature, use of cryptocurrency in scams frequently transcends traditional geographic borders. However, because this is true for all law enforcement entities, there is generally more international cooperation between large and small agencies in an attempt to combat illicit use of virtual currency. Many jurisdictions and agencies are willing to work cases in parallel or jointly with fellow law enforcement agencies, regardless of geographic location. TRM labs is happy to support public sector clients worldwide and would provide points of contact for cooperating law enforcement agencies where possible.

Additionally, scammers, unlike many other criminals, tend to be more brazen and use less operational security when traveling or admitting to their crimes. Therefore, there tends to be a greater opportunity for arrest and extradition either while traveling or even with countries that may not traditionally cooperate with Western law enforcement requests.

**Charging opportunities**

In addition to traditional fraud, theft, or misappropriation statutes, many of the schemes outlined above also trigger sentencing enhancements and increased charging opportunities. Scammers have been charged with computer crimes, extortion, racketeering, organized crime, money laundering, and a host of other crimes which could lead to significant sentences. There can also be significant sentencing enhancements based on age of victims, number of victims, using sophisticated schemes, moving money internationally, and aggregate dollar value of the schemes.

**Address:** A unique string of letters and numbers that represents a source or destination of a transaction on a blockchain. Cryptocurrency addresses can be thought of as similar to bank account numbers, as they can be shared publicly to receive funds.

**Attribution:** The process of labeling or assigning specific addresses to specific entities; (e.g. bc12345 is an address at Coinbase, a Virtual Asset Service Provider (VASP)).

**Bitcoin (BTC):** A decentralized virtual currency with transactions confirmed by open-source network nodes where transactions are recorded in the Bitcoin blockchain. Addresses are generally 27-34 alphanumeric, case sensitive characters, beginning with a 1, 3, or bc1 (e.g. 1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2).

**Blockchain:** A publicly available ledger of completed transactions between two or more cryptocurrency addresses that records transactions in code. Transactions are recorded in “blocks” of data that are then linked together on a “chain” of previous cryptocurrency transactions in chronological order.

**Block(chain) Explorer:** A web-based tool or application that allows users to explore and navigate a public blockchain network, sometimes with a graphing and linking function like TRM Labs’ Graph Visualizer. Its primary function is to provide users with a user-friendly interface to view and search for information about transactions, addresses, blocks, and other data stored on the blockchain.

**Blockchain Intelligence:** Enriched blockchain data, typically used for detecting and investigating illicit activity in virtual assets.

**Blockchain Tracing:** Tracking the source and destination of cryptocurrency transactions recorded on a particular blockchain.

**Counterparty:** The party that is on the opposite side of a transaction (e.g. if “A” sends bitcoin to “B,” “B” is the counterparty to “A”)

**Cryptocurrency:** A digital, encrypted, and decentralized medium of exchange. Unlike the U.S. dollar or the euro, there is usually no central authority that manages and maintains the value of a cryptocurrency. Instead, these tasks are broadly distributed among its users via the internet. Some cryptocurrencies, however, such as “stablecoins” do have a centralized authority confirming transactions.

**Crypto ATM/Kiosk:** The most common cash-to-crypto service. These terminals allow customers to insert fiat currency, buy cryptocurrency, and send it directly to a wallet. Crypto ATMs are marketed as tools to help individuals convert their money into cryptocurrency with maximum privacy and ease, more efficiently than at crypto exchanges. Crypto ATMs can be found in money service businesses, casinos, gas stations or any other business where one may find a traditional ATM.

**Ethereum:** A decentralized blockchain with smart contract functionality. Ether (ETH) is the native cryptocurrency on the platform, though there are thousands of other virtual currencies and applications that run on top of the Ethereum network, generally called “Layer 2” assets (which are completely separate virtual currencies from ETH). ETH addresses consist of 42 alphanumeric characters beginning with 0x (e.g. 0x71C7656EC7ab88b098defB751B7401B5f6d8976F).

**Direct/Indirect Exposure:** A measure of how directly proceeds may have traveled from one address to another. If “A” sent bitcoin directly to “B,” “A” has direct counterparty exposure to “B.” If “A” sent bitcoin to “B,” and “B” sent Bitcoin to “C,” “A” has direct counterparty exposure to “B” and indirect counterparty exposure to “C.”

## Know Your Customer (KYC)

**Information:** The real-world identification of an individual or business that an entity, including a crypto exchange or VASP, should collect as part of its compliance program. KYC may include information such as government-issued identification documents, contact information, and risk profiles.

**Liquidity Mining:** A process where individuals contribute their cryptocurrency to decentralized platforms or protocols to earn assets as rewards. Similar to getting interest by depositing your cash at a bank for the bank to use.

**Non-Fungible Token (NFT):** A type of digital asset that represents ownership or proves the authenticity of a unique item or piece of content, typically stored on a blockchain. Unlike cryptocurrencies such as bitcoin or ethereum, which are fungible and can be exchanged on a one-to-one basis generically (one bitcoin held in address 1bc12345 is worth the same as one bitcoin held in address 1bc54321), each NFT is distinct and cannot be exchanged on a like-for-like basis. NFTs can be used to represent one-of-a-kind digital assets like artwork, collectibles, virtual real estate, virtual goods in games, music, and videos. Even ownership of real world assets can be represented as an NFT.

**Private Key:** A unique, encrypted alphanumeric sequence that serves as the digital equivalent of a physical key to unlock and control digital assets. Having control of a private key allows the controller to manage or transfer the asset.

## Suspicious Activity Reports

### (SARs)/Suspicious Transaction Reports

**(STRs):** Government-mandated reports of potentially illicit or suspicious activities to regulatory authorities. SARs/STRs are a vital tool in combating money laundering, terrorist financing, fraud, and other financial crimes.

**Smart Contract:** A self-executing agreement or program written in code that is stored and executed on a blockchain (not dissimilar to an automatic futures contract). It enables parties to interact and conduct transactions in a transparent, automated, and secure manner without the need for intermediaries.

**Token:** A virtual currency asset that often runs on another virtual currency’s blockchain (e.g. an ERC-20 token such as USDT on Ethereum). Also sometimes called a “coin.”

**Transaction Hash:** Also known as a “Transaction ID”, this is a unique, alphanumeric sequence associated with a transaction on a blockchain. An investigator can identify specific transactions based on the transaction hash.

## Virtual Asset Service Provider (VASP):

A platform used to buy, sell, trade, or exchange virtual currency. VASPs, whether centralized or decentralized, may maintain attribution and transaction records which enable the investigator to identify the real-world controller of an address. Though VASPs are located throughout the world, many VASPs, regardless of physical location, will comply with law enforcement requests for production of records and freezes/seizures. “VASP” is the nomenclature used by international organizations such as the Financial Action Task Force (FATF). However, many blockchain investigators use the terms “VASP” and “exchange” synonymously (despite VASP technically including more than just centralized exchanges).

**Wallet:** A secure digital wallet used to store, send, and receive crypto. Wallets are distinct from addresses in that one wallet may hold multiple addresses, many times from multiple cryptocurrency assets. Wallets sometimes maintain two types of digital codes: the public key and the private key, allowing users to transact on blockchains. Wallets can be hardware, software, or even paper.

TRMLABS.COM