SOP ON INVESTIGATION PROCESS/ METHODOLOGIES FOR CRYPTOCURRENCY RELATED CYBER CRIMES

(August, 2021)

NATIONAL CYBER CRIME RESEARCH & INNOVATION CENTRE (NCR&IC)

Modernization Division

BUREAU OF POLICE RESEARCH AND DEVELOPMENT

Ministry of Home Affairs, Government of India

SoP on Investigation Process/ Methodologies for Cryptocurrency related Cyber Crimes

National Cyber Crime Research & Innovation Centre (NCR&IC)

Modernization Division

Bureau of Police Research & Development

New Delhi

Disclaimer

- This document is not a substitute for existing manuals available in the States/UTs. It is only a guide for awareness purpose. In case of any conflict, local manual/ practice may prevail.
- BPR&D does not promote any tool/software of a particular vendor. All the tools and software mentioned in this manual are for illustration purpose only.
- Wherever any Image/graphics/flowchart is taken from other sources, the same has been duly acknowledged.

वरुण सिंधु कुल कौमुदी, भा.पु.से.
महानिदेशक

VSK Kaumudi, IPS
Director General
Tel. : 91-11-26781312 (0)
Fax : 91-11-26781315
Email : dg@bprd.nic.in

पुलिस अनुसंधन एवम् विकास ब्यूरो
गृह मंत्रालय, भारत सरकार
राष्ट्रीय राजमार्ग-8, मडिपालपुर,
नई दिल्ली-110037

Bureau of Police Research & Development
Ministry of Home Affairs, Govt. of India
National Highway-8, Mahipalpur,
New Delhi-110037

Message

The setting up of the National Cyber Crime Research & Innovation Centre (NCR&IC) at the BPR&D Hqrs.and its branch, the National Cyber Crime Research, Innovation and Capacity Building, at the CDTI, Hyderabad, has been a major technological milestone in the cyber research and training capabilities of the BPR&D. The NCR&IC, as part of the umbrella scheme of the Indian Cyber Crime Coordination Centre (14C), MHA, has been striving countinuously to strengthen and augment the capacity of Law Enforcement Agencies (LEAs) in their efforts of Cyber Crime prevention and investigation.

I am happy that NCR&IC professionals have come up with the following four booklets to address the urgent need for awareness related to Cyber Crimes, keeping in mind the skill set required by the police officers in the investigation of Cyber Crimes:

- Emerging Cyber Crimes in India - A Concise Compilation
- First Responder Handbook - Computer System Acquisition
- SOP on Investigative Process/Methodologies for Cryptocurrency related Cyber Crimes
- Manual on Social Media Intelligence (SOCMINT) for LEAs

The above manuals/SOPs are result of the sincere efforts of Dr. Karuna Sagar, IPS, IG (Modernization), Sh. B. Shanker Jaiswal, IPS, DIG (Mod), Dr. M. M. Gosal, SSO (T) and NCR&IC professionals/experts, namely, Dr. Pankaj Choudhary, Sh. Gourav Chaurasia, Sh. M. Krishna Chaitanya and Sh. Farhan Sumbul, BPR&D. I record my deep appreciation for their hard work.

I believe, these booklets will guide the police officers in understanding the Cyber Crimes of various categories, including the modus operandi of cyber criminals, Data Acquisition in different scenarios, Methodology for Investigating Cryptocurrency and Social Media Platform, etc.

(V.S.K.Kaumudi)

Place: New Delhi

नीरज सिन्हा, भा.पु.से.
अपर महानिदेशक

Neeraj Sinha, IPS
Additional Director General

Tel.: + 91 11 26781341 • Fax: 91 11 26782201
Email: adg@bprd.nic.in • Website: www.bprd.nic.in

पुलिस अनुसंधान एवम् विकास ब्यूरो
गृह मंत्रालय, भारत सरकार
राष्ट्रीय राजमार्ग-8, महिपालपुर,
नई दिल्ली-110037

Bureau of Police Research & Development
Ministry of Home Affairs, Govt. of India
National Highway-8, Mahipalpur,
New Delhi-110037

Message

Technology is often value neutral. It can be used effectively by friends and foes alike. On occasions, the rapid strides by technology, especially in the domain of cyber-space, threatens to outpace the skills of inadequately trained professionals, especially at the cutting edge.

BPR&D, with its motto of 'Promoting Good Standards and Practices', has often bridged the information gap for the LEAs, with its thoughtful seminars and publications. It gives me great pleasure that the National Cyber Research & Innovation Centre (NCR&IC) professionals are putting together 04 significant compilations, including 'Emerging Cyber Crimes in India – A Concise Compilation'; 'First Responder Handbook – Computer System Acquisition'; 'SOP on Investigative Process/Methodologies for Crypto-currency related Cyber Crimes'; and 'Manual on Social Media Intelligence (SOCMINT) for the LEAs'.

The team of the Modernization Division of the BPR&D, led by Dr. Karuna Sagar, IPS, IG, Shri B S Jaiswal, IPS, DIG, Dr. Manjunath M Gosal, SSO (T), Dr. Sarabjit kaur, Dr. Pankaj Choudhary, Sh. Gourav Chaurasia, Sh. M. Krishna Chaitanya and Sh. Farhan Sumbul, are deserving of our appreciation for the publications.

I trust the Investigating Officers, particularly at the cutting edge, would find these compilations useful in their day to day professional lives.

(Neeraj Sinha)

Place: New Delhi.

डॉ. करुणा सागर, भा.पु.से.
महानिरिक्षक/निदेशक (आधुनिकीकरण)

Dr. Karuna Sagar, IPS
Inspector General/Director (Modernisation)

Tel. : 91-11-26782023
91-11-26782030 (F)
Email : igmod@bprd.nic.in

पुलिस अनुसंधन एवम् विकास ब्यूरो
गृह मंत्रालय, भारत सरकार
राष्ट्रीय राजमार्ग-8, महिपालपुर,
नई दिल्ली-110037

Bureau of Police Research & Development
Ministry of Home Affairs, Govt. of India
National Highway-8, Mahipalpur,
New Delhi-110037

Executive Summary

States/UTs are primarily responsible for the prevention, detection, investigation and prosecution of new-age cryptocurrency-related crimes through their law enforcement machinery. As more and more users access the internet and are embracing technology the cyber criminals are looking at crypto-currencies for transactions. With the gaining popularity and awareness ampongst the people of India with respect to cryto-currencies such as Bitcoin, Ripple, Dogecoin, etc., many have started investing part of their time and money in these virtual currencies.

In India, crypto-currency has been understood as a from digital/ virtual currency generated through a series of written computer codes that rely on cryptography which is encrypted and is thus independent of any central issuing authority per se. It is facilitated through blockchain technology and has emerged as a person-to-person issuance and transaction system that uses private and public keys that enable authentication and encryption for secure transactions.

The "SOP on investigation process/methodologies for Cryptocurrency related crimes" is also one of the intiatives by the NCRIC, the BPR&D. This manual is an introduction to crypto-currencies and various types of cyber crimes related to it. It further covers easy to follow steps about the seizure methods for crypto-currency with fowcharts and initial investigative methodologies related to blockchain. The booklet also includes procedure of seizing bitcoins, and ways to analyse bitcoin addresses using OSINT to get started with the investigation.

The SOP conncludes with the recent developments in technology and the challenges that lay achead while investigating crypto-currency crimes.

The major contribution to this booklet is made by Sh. M. Krishna Chaitanya, Digital Forensic Expert NCR&IC, BPR&D in successfully bringing out this booklet

18.8.2021

(Dr. Karuna Sagar)

Place: New Delhi

Contents

ABBREVIATIONS

SOP - Standard operating procedure

OSINT- Open Source Intelligence

LEA- Law Enforcement Agencies

BTC - Bitcoin

POW - Proof of work

POC - Proof of Concept

1 Introduction

In 2008, Satoshi Nakamoto released a white paper titled, "Bitcoin: A Peer-to-Peer Electronic Cash System.". People still do not know who the actual creator is or anything about him or her. Satoshi Nakamoto could be one person, male or female, or a group of individuals.

Bitcoin then was relatively cheap as compared to today and it was slowly being accepted by the cyber world Bitcoin used to be mined, won in games for free. slowly as and when the price started rising it was being exchanged as a currency given the nature of the currency it was particularly popular in the dark web markets, this pseudo-anonymous nature of Bitcoins made it an automatic choice for cybercriminals.

In this booklet, we are going to go get to know what is cryptocurrency, crimes related to cryptocurrency how to seize bitcoins, and since this is introductory what are some ways to analyze bitcoin addresses using OSINT to get started with the investigation. The law related to cryptocurrency in India and the recent developments as of the date.

Finally, conclude with the recent developments in technology and the challenges that lay ahead while investigating cryptocurrency crimes .

2 What is cryptocurrency?

- Cryptocurrencyis trillion-dollar industry globally. Many big bank and billionaires have already invested in crypto
- No democracyglobally have banned cryptocurrency, something which is decentralised cannot be banned
- Crypto and bitcoin sounds like complex concepts but millions of people in India aremaking money by buying and selling cryptocurrencies

The word CryptoCurrency is a combination of the words Crypto – meaning 'Hidden' and the word Currency meaning – 'a system of money in a country. Hence Cryptocurrency is a pseudo-anonymous form of payment. One important feature of Cryptocurrencies is that they are decentralized and no bank or government has control over it. Cryptocurency transactions have no territorial jurisdiction and can be accessed anywhere in the world without any standard legal procedures.

2.1 Characteristics

A) Peer to peer

Cryptocurrency uses a peer-to-peer system in which, users are allowed to send transactions to one another without using an intermediary unlike in a traditional banking system.

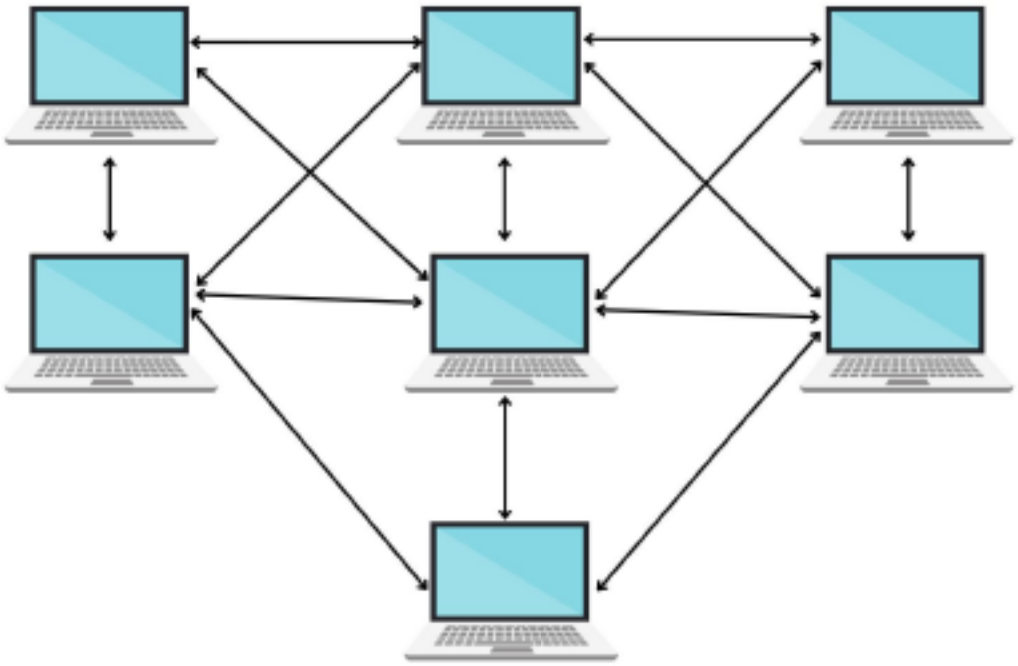


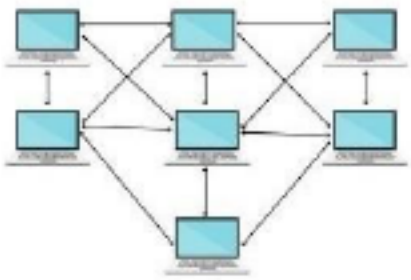
Figure 1 – Structure of cryptocurrency

B) Public

Each person using cryptocurrency has access to a digital, public record (ledger) of all transactions the source and destination can be seen on the respective explorers of the currency.

C) No Central Server

The peer-to-peer system eliminates the need for a central server or a central authority to track money going in and out as is used in traditional currency. Cryptocurrency uses a decentralized network of computers or nodes. Each node maintains a copy of the ledger (blockchain)



There is no Centralized servers in cryptography its Decentralized

2.2 Some Common Terms - Proof of Work, Proof of Stake

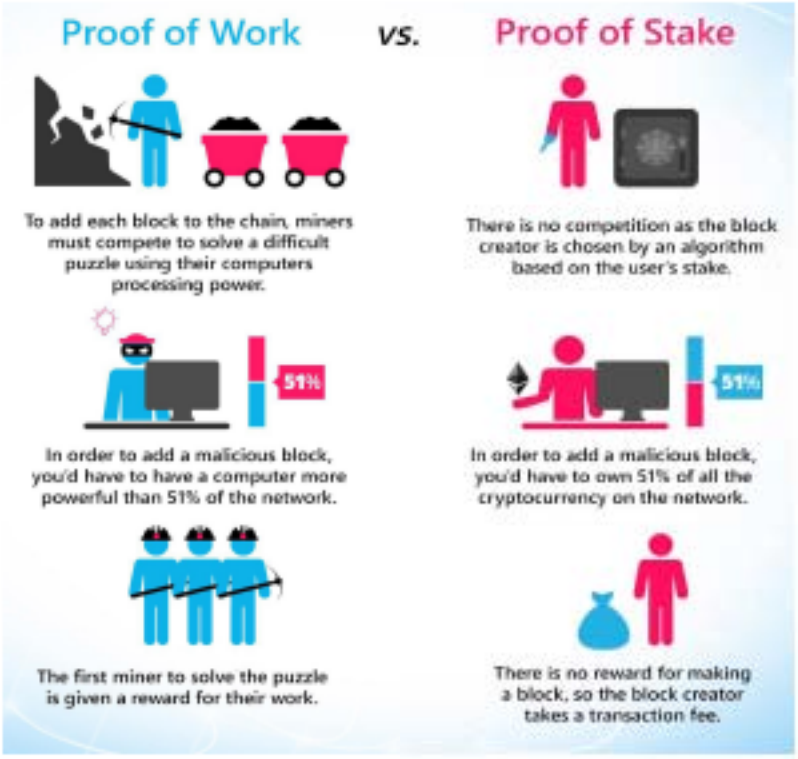


Figure 2 – Proof of Work vs Proof of Stake

Source: https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/

A common term one would come across while understanding CryptoCurrencies is "Proof of work" and "Proof of stake"

Proof of Work: It is the original consensus algorithm in a BlockChain network. Just as in normal life we need to work to earn every penny, most cryptocurrencies such as Bitcoin, Bitcoin Cash need Proof of Work before being credited to anyone. This Proof of work is the value of a Mathematical function to be guessed by an Intensive Graphical Unit or Computer system before they can add a new block to the existing chain.

Proof of Stake – The Proof of Stake is another consensus mechanism wherein to write the next block to the existing chain, several factors such as Wealth, Age, Number of days currency held for, etc. are taken into account. Cryptocurrencies such as Ethereum work on this concept.

Transaction Verification

Once a transaction is complete, a person called a miner will verify that the transaction is legitimate, which involves solving a cryptography puzzle to ensure that no one is spending money they do not have. The system runs on consensus, meaning that once a consensus of at least 51% agrees that a transaction is valid, it is confirmed.

A miner can be anyone, provided they have the proper high-end computer equipment.

The miner will receive a transaction fee for completing this work.

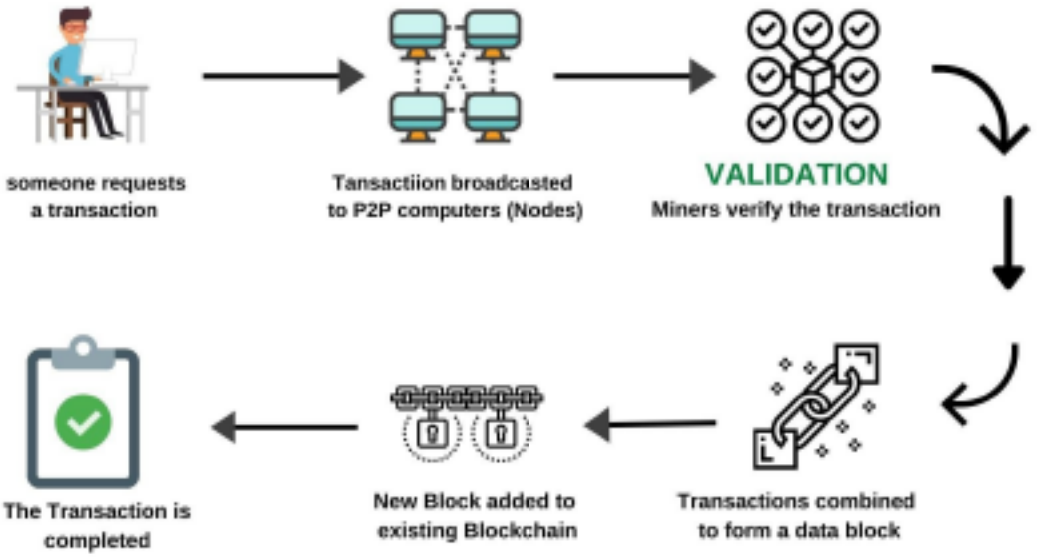


Figure 3 – Transaction of Cryptocurrencies

Source wikipedia

3. Types of Cryptocurrencies

After the invention of bitcoin, many blockchain experts came up with concepts for various coins such as Etherium, Binance coin, Litecoin, Dash, Ripple, and Privacy centric coins such as Monero, Zcash

Table 1 – List of popular Cryptocurrencies

	Bitcoin (BTC)	❖ Bitcoin, launched in 2009, was the first of a new kind of asset called cryptocurrency, a decentralized form of digital cash that eliminates the need for traditional intermediaries like banks and governments to make financial transactions. ❖ Bitcoin is powered through a combination of peer-to-peer technology network of individuals, much like the volunteer editors who create Wikipedia — and software-driven cryptography, the science of passing secret information that can only be read by the sender and receiver.
	Ethereum (ETH)	❖ Ethereum is a decentralized software platform that enables Smart Contracts and Decentralized Applications (DApps) to be built and run without any downtime, fraud, control, or interference from a third party. ❖ The goal behind Ethereum is to create a decentralized suite of financial products that anyone in the world can have free access to, regardless of nationality, ethnicity, or faith. ❖ In 2021 Ethereum plans to change its consensus algorithm from proof-of-work to proof-of-stake. This move will allow Ethereum's network to run itself with far less energy as well as improved transaction speed.
	Binance Coin (BNB)	❖ Binance Coin is a utility cryptocurrency that operates as a payment method for the fees associated with trading on the Binance Exchange. Those who use the token as a means of payment for the exchange can trade at a discount. Binance Coin's blockchain is also the platform that Binance's decentralized exchange operates on. The Binance exchange was founded by Changpeng Zhao and the exchange is one of the most widely used exchanges in the world based on trading volumes.

	Litecoin (LTC)	v Litecoin, launched in 2011, was among the first cryptocurrencies to follow in the footsteps of Bitcoin and has often been referred to as "silver to Bitcoin's gold." v It was created by Charlie Lee, an MIT graduate, and former Google engineer. ❖ Litecoin is based on an open-source global payment network that is not controlled by any central authority and uses "scrypt" as a proof of work, which can be decoded with the help of CPUs of consumer-grade. *Although Litecoin is like Bitcoin in many ways, it has a faster block generation rate and hence offers a faster transaction confirmation time.*
	Dash (DASH)	❖ Dash (Symbol: DASH) was created in January 2014 to be the most user-friendly and scalable cryptocurrency. Formerly known as Xcoin and Darkcoin, it was designed to protect the anonymity of its users while also facilitating almost instant transactions. Dash was designed to improve on Bitcoin's perceived flaws, especially in terms of transaction times and privacy. Dash's creators view it as being the next logical step towards fully digital cash.

	Ripple (XRP)	❖ While Bitcoin is a digital currency intended as a means of payment for goods and services, Ripple is a payment settling, currency exchange, and remittance system intended for banks and payment networks. The idea is to provide a system for direct transfer of assets (e.g. money, gold, etc.) ❖ Transactions are settled within seconds on the Ripple network even though the platform handles millions of transactions frequently. … As of August 2019, Ripple was the third-largest cryptocurrency by market cap of $13.37 billion, following Bitcoin (BTC) at $205.03 billion, and Ethereum (ETH) at $24.18 billion
	Monero (XMR)	❖ Monero is a secure, private, and untraceable currency. This open-source cryptocurrency was launched in April 2014 and soon garnered great interest among the cryptography community and enthusiasts. The development of this cryptocurrency is completely donation-based and community-driven. Monero has been launched with a strong focus on decentralization and scalability, and it enables complete privacy by using a special technique called "ring signatures."

	Cardano ADA	❖ Cardano is a Switzerland-based Cryptocurrency launched on 27 September 2017. Cardano was developed with the idea to run a Public Blockchain platform for smart contracts. Cardano's internal currency is called Ada.
	Polkadot	❖ Polkadot is a heterogeneous multi-chain interchange and translation architecture that enables customized side-chains to connect with public blockchains. Polkadot's first token went on sale on 27 October 2017
	Tether	❖ It is not bitcoin or ether, but tether which is the most traded cryptocurrency today. Commonly denominated as USDT, the tether is a stable currency, which can be redeemed for a dollar. In other words, if one holds 100 USDT, they can redeem it for $100. It was founded in 2014
	Uniswap	❖ Uniswap is a decentralized finance protocol that is used to exchange cryptocurrencies. Uniswap aims to keep token trading automated and completely open to anyone who holds tokens while improving the efficiency of trading versus that on traditional exchanges.
	Chainlink	❖ Chainlink (LINK) is a decentralized oracle network that aims to connect smart contracts with data from the real world. Chainlink was developed by Sergey Nazarov, with Steve Ellis as the other co-founder.
	Bitcoin Cash	❖ Bitcoin Cash is a peer-to-peer electronic cash system that aims to become sound global money with fast payments, micro fees, privacy, and high transaction capacity (big blocks). In the same way that physical money, such as a dollar bill, is handed directly to the person being paid, Bitcoin Cash payments are sent directly from one person to another.

	USD Coin	❖ USD Coin (known by its ticker USDC) is a stable coin that is pegged to the U.S. dollar on a 1:1 basis. Every unit of this cryptocurrency in circulation is backed up by $1 that is held in reserve, in a mix of cash and short-term U.S. Treasury bonds.

	Stellar	❖ Stellar is an open network that allows money to be moved and stored. When it was released in July 2014, one of its goals was boosting financial inclusion by reaching the world's unbanked — but soon afterward, its priorities shifted to helping financial firms connect through blockchain technology.
	Wrapped Bitcoin	❖ Wrapped Bitcoin is a tokenized version of Bitcoin (BTC) that runs on the Ethereum (ETH) blockchain. WBTC is compliant with ERC-20 — the basic compatibility standard of the Ethereum blockchain — allowing it to be fully integrated into the latter's ecosystem of decentralized exchanges, crypto lending services, prediction markets, and other ERC-20-enabled decentralized finance (DeFi) applications.
	Dogecoin	❖ Dogecoin (DOGE) is based on the popular "Doge" Internet meme and features a Shiba Inu on its logo. The open-source digital currency was created by Billy Markus from Portland, Oregon, and Jackson Palmer from Sydney, Australia, and was forked from Litecoin in December 2013. Dogecoin's creators envisaged it as a fun, light-hearted cryptocurrency that would have greater appeal beyond the core Bitcoin audience since it was based on a dog meme. Tesla CEO Elon Musk posted several tweets on social media that Dogecoin is his favorite coin.
		Tron: (TRX) TRON is a Blockchain with a crypto currency native to the system, known as TRX. Justin Sun founded the crypto currency in 2017. The block chain Tron is separate Crypto Currency block chain. Tron holds decentralised exchanges across the world. High throughput is achieved by improving the TPS in TRON, which has surpassed Bitcoin and Ethereum, to a daily-use practical degree. More reliable network structure, user asset, intrinsic value and a higher degree of decentralization consensus come with an improved rewards distribution mechanism. Tron is being used for purchasing crypto currency tokens like USDT, ETHERIUM etc .

From which Crypto exchange, the KYC or due diligence of the wallets account has been done ?

4. Transaction Methodology

Now let's see how a transaction takes place. To complete a cryptocurrency transaction, users need a public and private key.

- *The public key is equivalent to an account number.*
- *The private key is like a PIN or password that allows the user to spend their cryptocurrency.*

Public and private keys are comprised of a long string of numbers and letters.

Public Key

Like an account number, this is visible to anyone with Internet access when transactions are added to the blockchain.

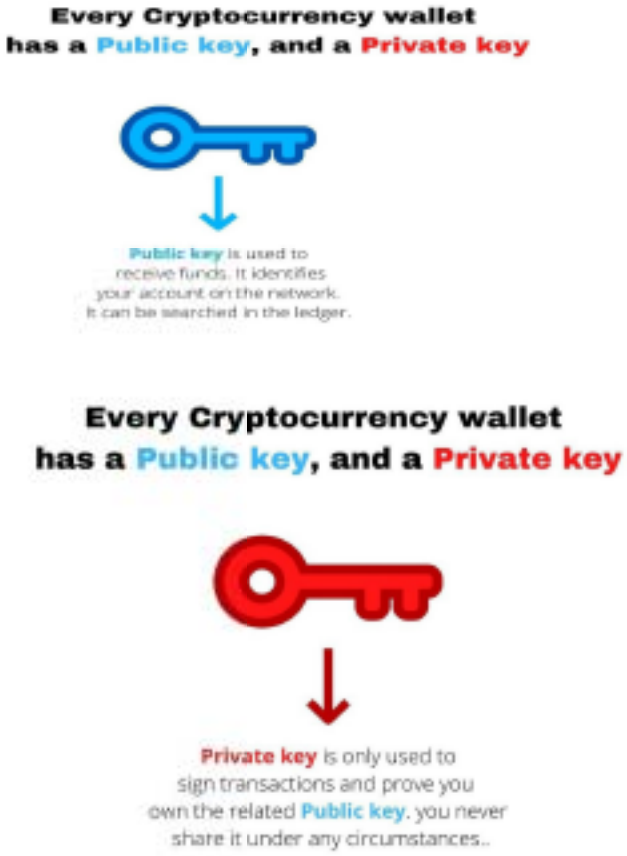


Figure 4 – Concept of Public and Private key

The password allows users to access the funds in their accounts.

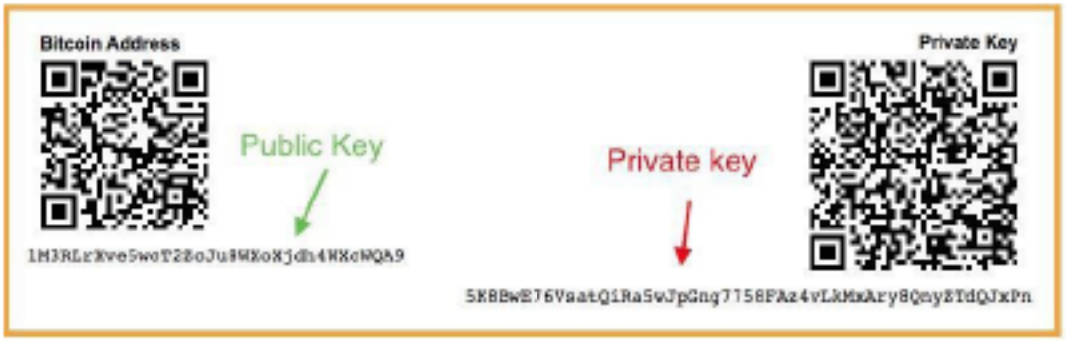


Figure 5 – Public and Private key and bitcoin Addresses

Source: https://blog.coinswitch.co/how-to-protect-your-crypto-holdings-with-a-private-wallet-ad2c6070778d

Protecting the Private Key

To protect cryptocurrency, users must protect their private keys. Phishing and malware can be used to steal private keys. If a private key is stored on a device with Internet access, the user is at greater risk of cryptocurrency theft.

Note: LEAs should be aware of scam coins. A developer may create a new currency and offer investors an opportunity to "get rich quick." But in reality, they use this scheme to take advantage of novice investors.

Users can store their public and private keys in a variety of digital and non-digital wallets; most users will use a digital wallet.

Using a wallet is vital for cryptocurrency users because it allows them to store their private keys in a safe place. Though it is important to keep track of your electronic wallet, there is a backup should something happen to it. This is called a recovery seed.

Recovery Seed

A recovery seed is a unique and random series of words that are recorded when establishing an electronic wallet. If the wallet is misplaced, damaged, lost, or stolen, the recovery seed allows you to regenerate the wallet, including the public and private keys.

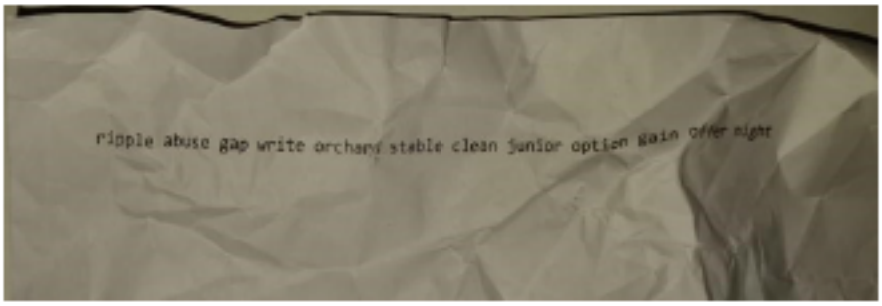


Figure 6 – Seed password example

5. Types of wallets

A) Websites

A website is useful because it allows users to access their cryptocurrency on any web-enabled device. Although an online account is at risk of being hacked, it is convenient for small quantities of cryptocurrency.

Figure 7 – Website Wallet

B) Apps

As an online account through a website, storing cryptocurrency through an app is convenient for on-the-go spending. Like websites, because apps are connected to the Internet, you are at a higher risk of being hacked than more disconnected wallets.

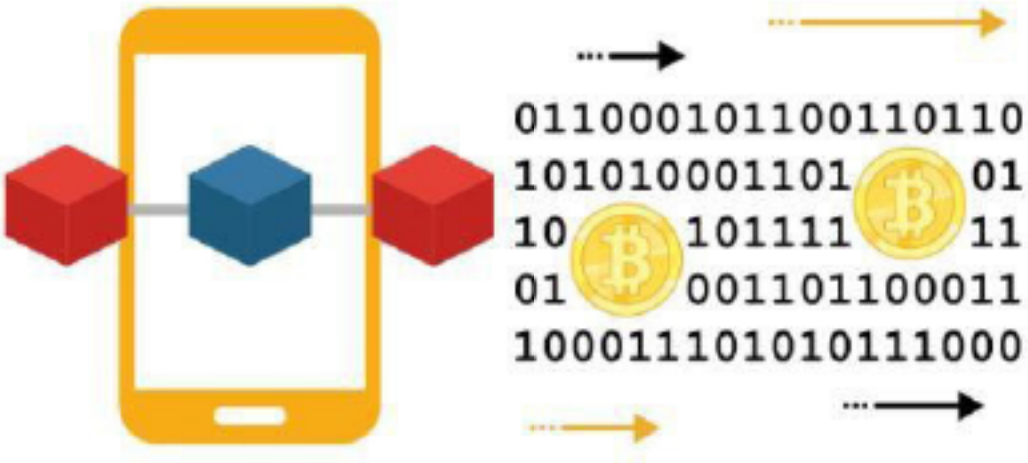


Figure 8 – Mobile wallet

The User Interface of two of the most widely used Wallets used for managing and storing cryptocurrencies are as below :

Exodus -

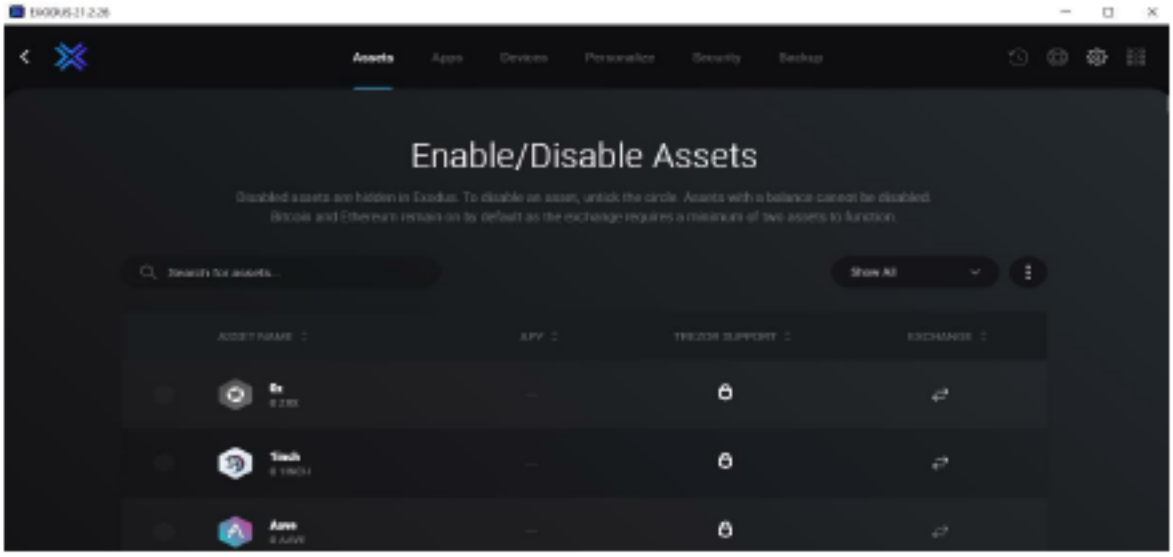


Figure 9 – Exodus wallet user inteface

Electrum

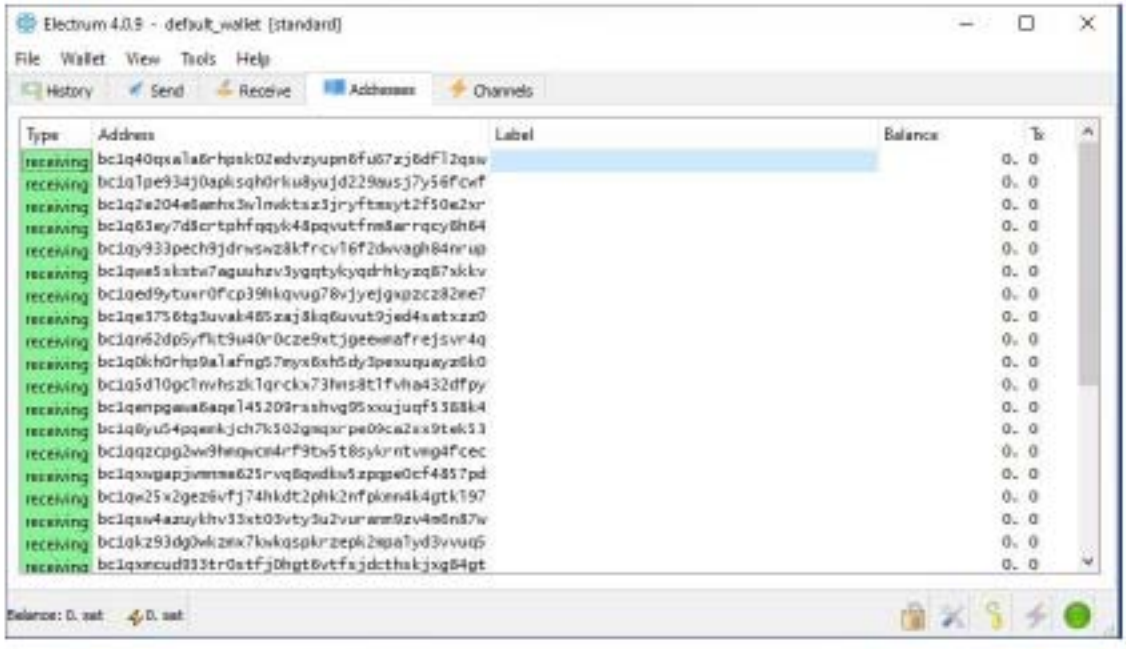


Figure 10 – Electrum wallet user interface

Computer Hard Drive

Both public and private keys may be stored through a computer program. If the computer has Internet access, the private key could be hacked, but hard drives have the potential to be more secure than apps or websites since computers can be disconnected from the Internet.

Figure 11 – A hardware wallet

C) Hardware Wallets

Hardware Wallets, specifically designed to store cryptocurrency keys, are more secure than other types of digital cryptocurrency wallets because they can be removed from the computer, keeping them safe from hackers. Types of Cold wallets: Eg: hardware wallets (Trezor and SafePal) and Paper wallets.

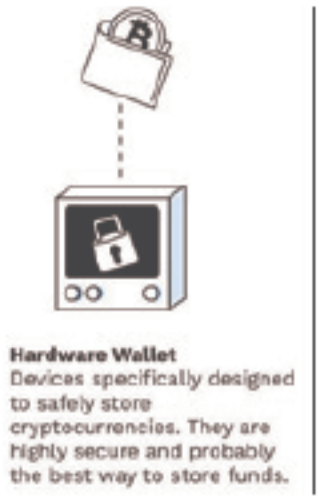


Figure 12 – Collection of H/W wallets

D) Paper Wallet

Paper wallets have a quick response (QR) code containing a user's public and private keys. These wallets are the most secure way of storing cryptocurrency since they are not electronic and, therefore, cannot be hacked. However, if someone steals a paper wallet, they will have the public and private keys to access the account.

Figure 13 – Examples of paper wallets

E) Web Browser

A web browser may have links in its history of cryptocurrency sites where a wallet is kept. Use keywords when searching for cryptocurrency websites, such as block, chain, coin, and wallet. Examples of cryptocurrency websites include https://coinbase.com, https://coinmarketcap.com, and https://upbit.com.

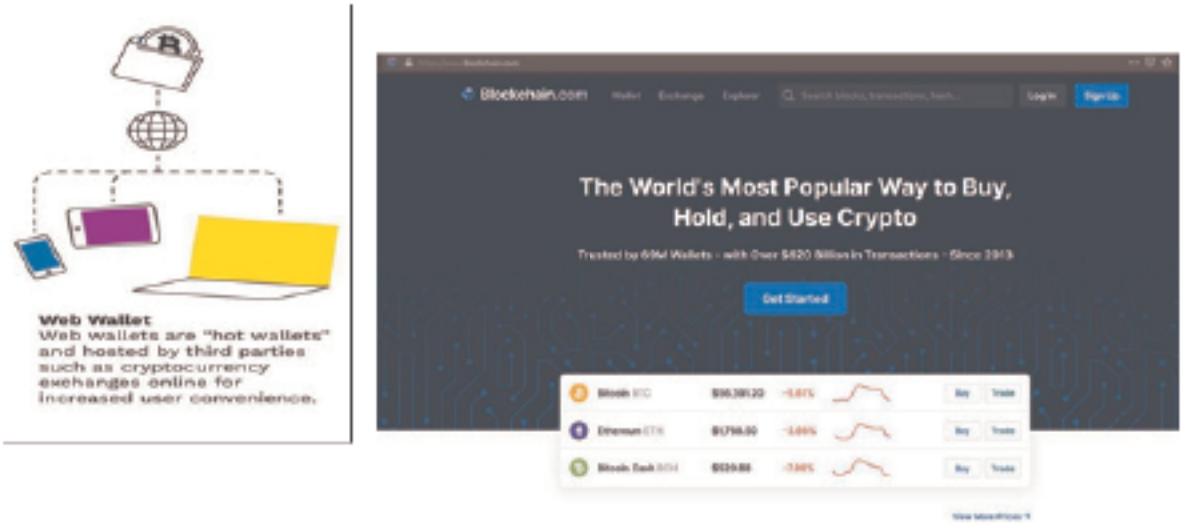


Figure 14 – Browser based wallet

F) Smartphone

Examples of cryptocurrency apps that may be found on a smartphone include Blockchain Wallet, Blockfolio, Coincap, and Bitcoin Balance.

G) Paper Wallet

You may suspect that a piece of paper is a cryptocurrency wallet if QR codes are present. Note that QR codes are used for more than just cryptocurrency. Further investigation will help you determine the true purpose of the paper.

F) Anonymity-Enhanced Cryptocurrencies

New cryptocurrencies called anonymity-enhanced cryptocurrencies are significantly more anonymous than earlier cryptocurrencies. Examples include Z-cash, Dash, Verge, and Monero.

Unlike Bitcoin, altcoins lack a public ledger, which makes it more challenging to tie an individual to a specific transaction. However, Bitcoin is still the number one cryptocurrency among criminals because it is much easier to convert to cash.

Despite the best efforts of law enforcement, criminals continue to devise new ways to operate to try to keep an edge and the use of cryptocurrency is no different.

G) Hot Wallets

i) Desktop wallets like electrum and Armory

ii) Mobile walletslike Edgeand Trust wallet

iii) Hybrid Walletslike BTC Pay and Blockchain

H) Cold Wallets: Hardware wallets, like Trezor, Safepal, Ledger nano and paper wallets.

6. Role of Cryptocurrency in cybercrime

Cryptocurrency is being adopted widely for its decentralization and anonymous nature. This pseudo-anonymous nature of cryptocurrency mainly bitcoin makes it an automatic choice for using it as means of currency for nefarious purposes dark web markets, ransomware attacks, crypto-jacking, money laundering, tax evasion, etc. The crimes discussed above are directly facilitated by using crypto transactions whereas some crimes involve crypto directly such as Ponzi schemes involving cryptocurrency exchanges, theft of cryptocurrency, etc.

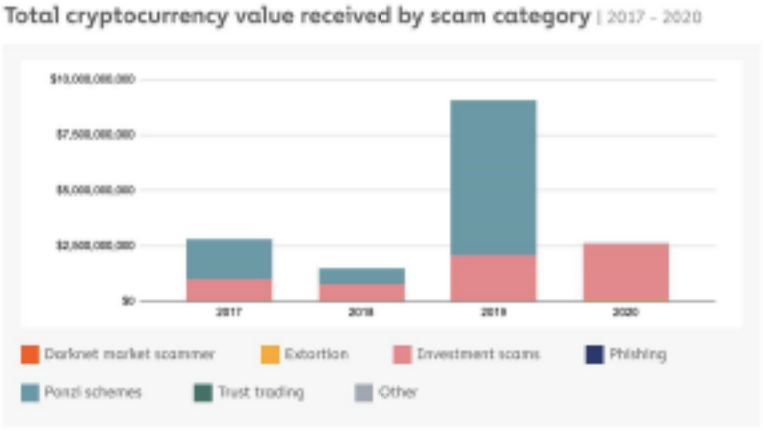


Figure 15 – Statistics from Chain Anamlysis

Source: https://www.chainalysis.com/

Investment scams and Ponzi schemes were most rampant and most amounts of money in cryptocurrency were received by the bad actors. These statistics prove this point.

Risk Categories of wallets are decided on the basis of data sets and previous transaction records and the wallets are rated within the range of 1 to 10. As much as high rating, the wallet is marked as 'High Risk' category. The Terminology used for categorising the wallets are; ATM, Child Abuse, Gambling, Dark Net, High Risk , P2p, Exchange, Mixture cluster, Terror Financing, Ransom etc.

Timeline of Crypto scams world over

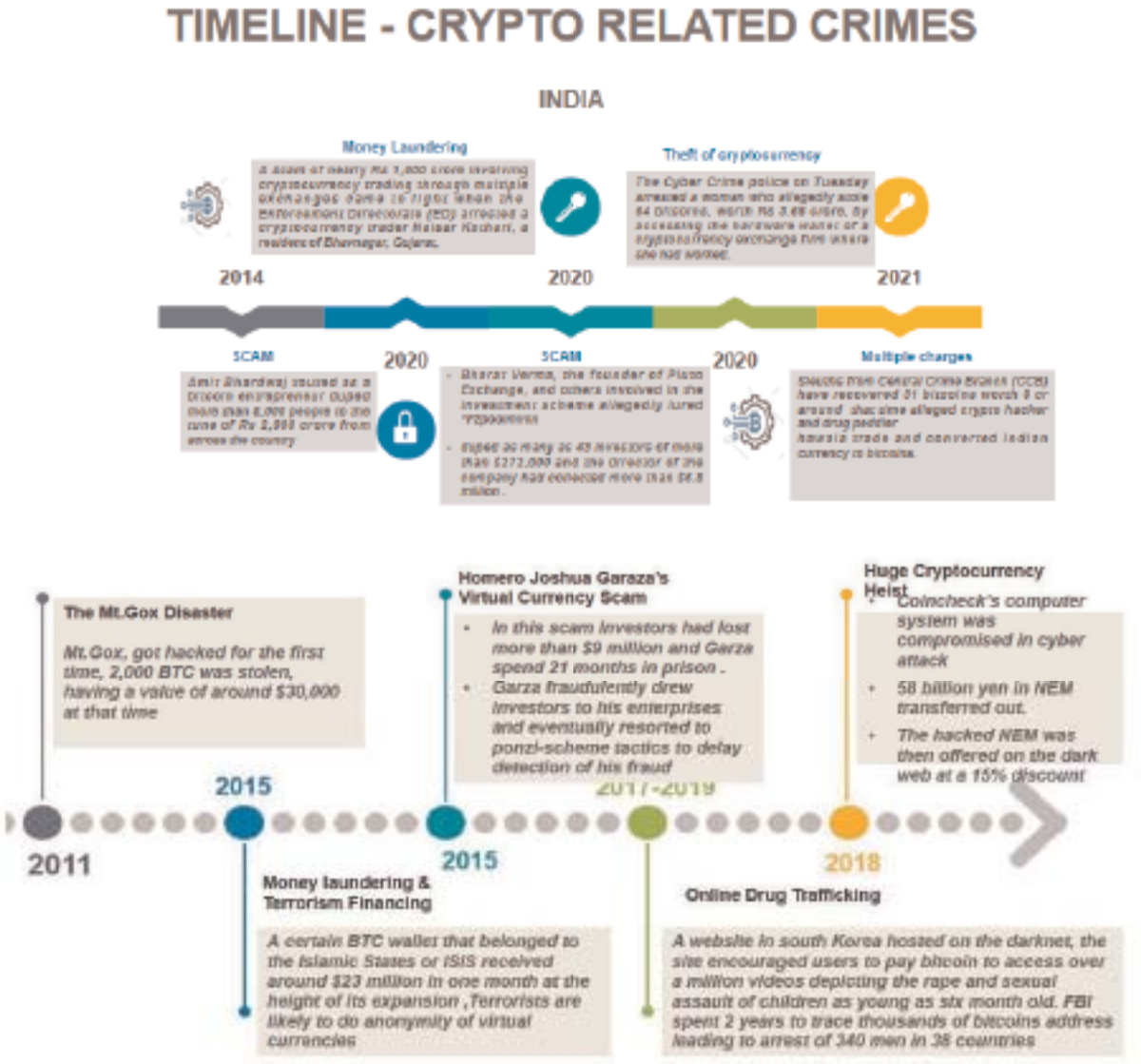


Figure 16 – Timeline of Cryptoscams (world over and india)

A) Contraband Transactions

The dark web is an online black market where illegal goods and services are sold. It thrives because cryptocurrencies provide anonymity to buyers and sellers. Buyers can use cryptocurrency to purchase weapons, drugs, and even hitman services with less fear of being caught.

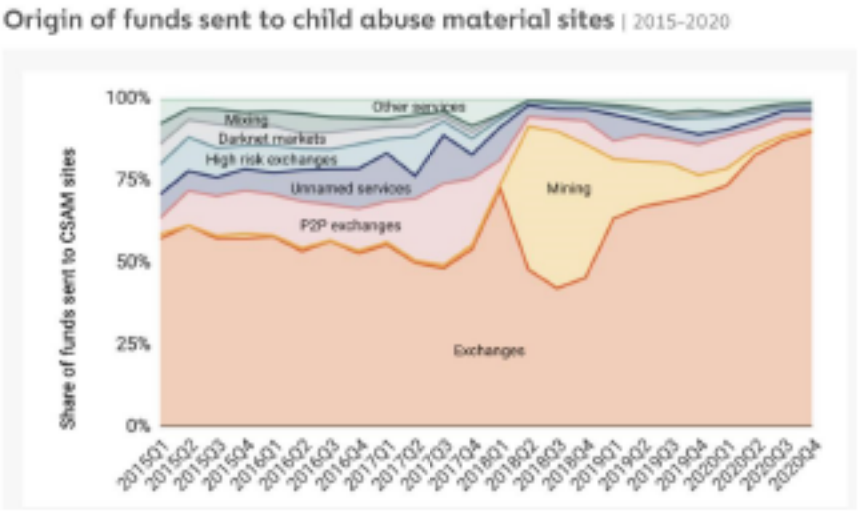


Figure 17 – Statistics for share of funds sent to CSAM

Source: https://www.chainalysis.com/

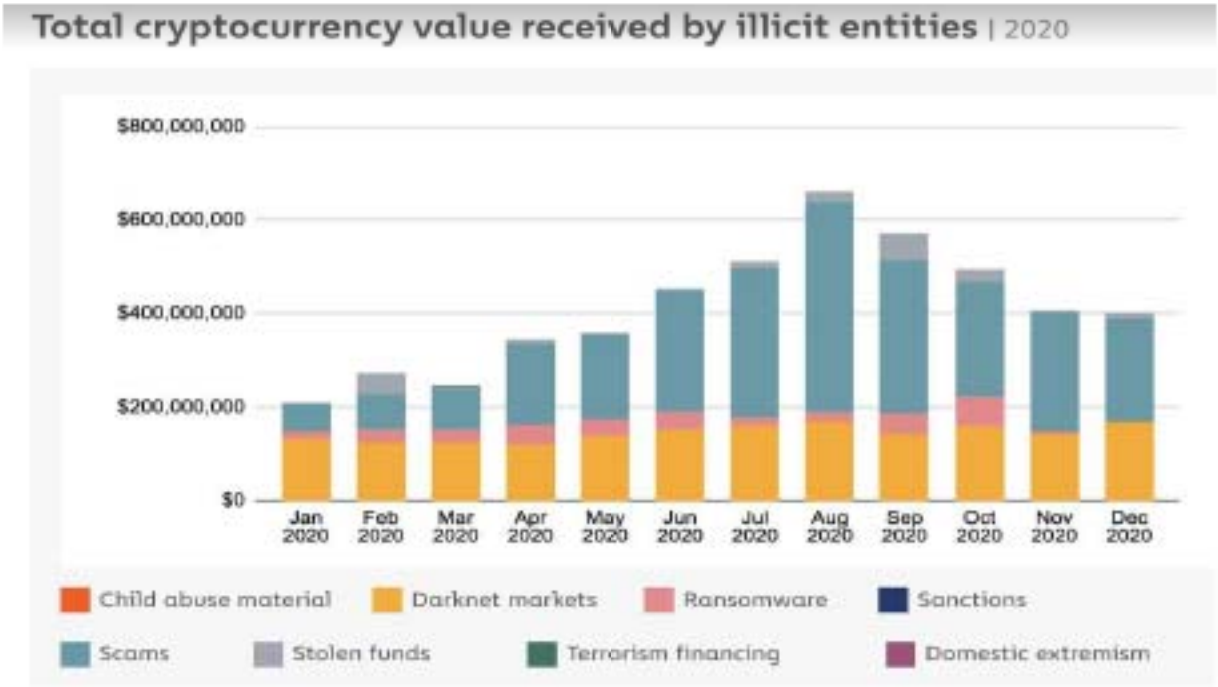


Figure 18 – Statistics for cryptocurrencies received by illicit entities

Source: https://www.chainalysis.com/

B) Extortion and Ransomware

Cryptocurrency is sometimes used as payment for extortion because the money trail is so difficult to trace.

A common extortion tool is ransomware. Ransomware is software that takes over a computer and does not allow access to its files until a ransom is paid, usually in cryptocurrency. Victims of ransomware range from individuals to entire companies.

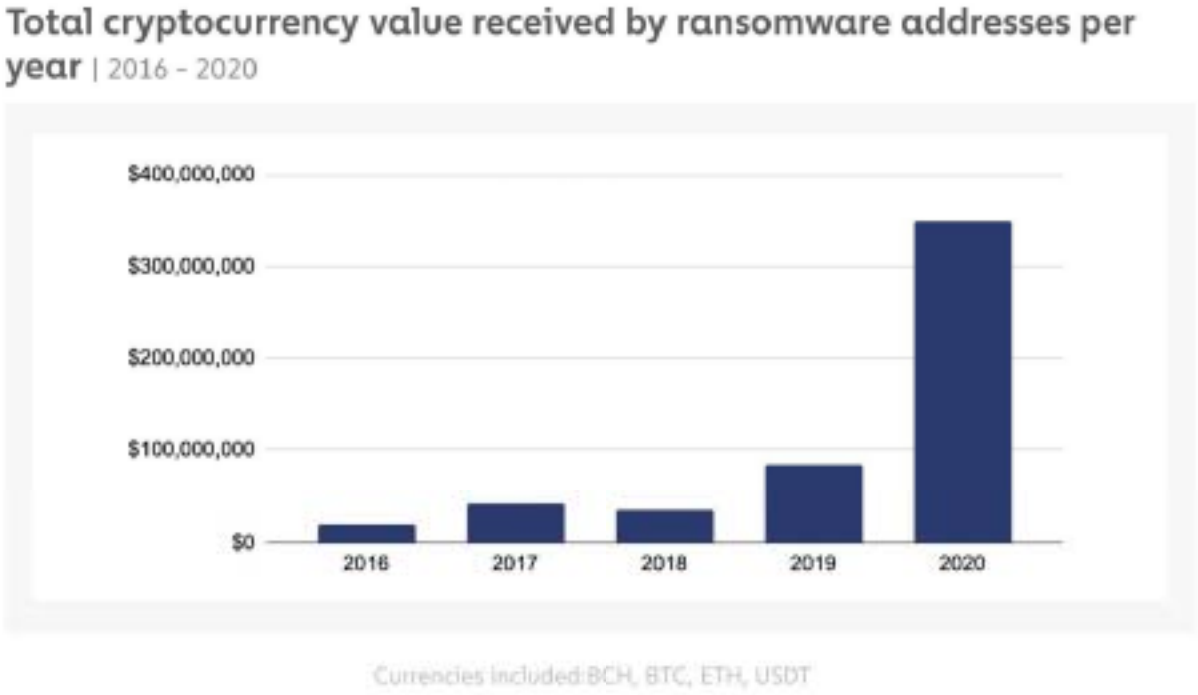


Figure 19 – Statistics from Chain analysis

Source: https://www.chainalysis.com/

C) Tax Evasion and Money Laundering

The pseudo-anonymous nature of cryptocurrencies and the ease and speed that they can be moved from one person to another, anywhere in the world, make them attractive to people wishing to launder money or evade taxes.

D) Fraud and Scams

As you learned previously, scam coins are a way to illegally take advantage of novice investors. This is often done through an Initial Coin Offering or ICO. ICOs are a way for people to invest in a new cryptocurrency venture. Some are legitimate while others are scams.

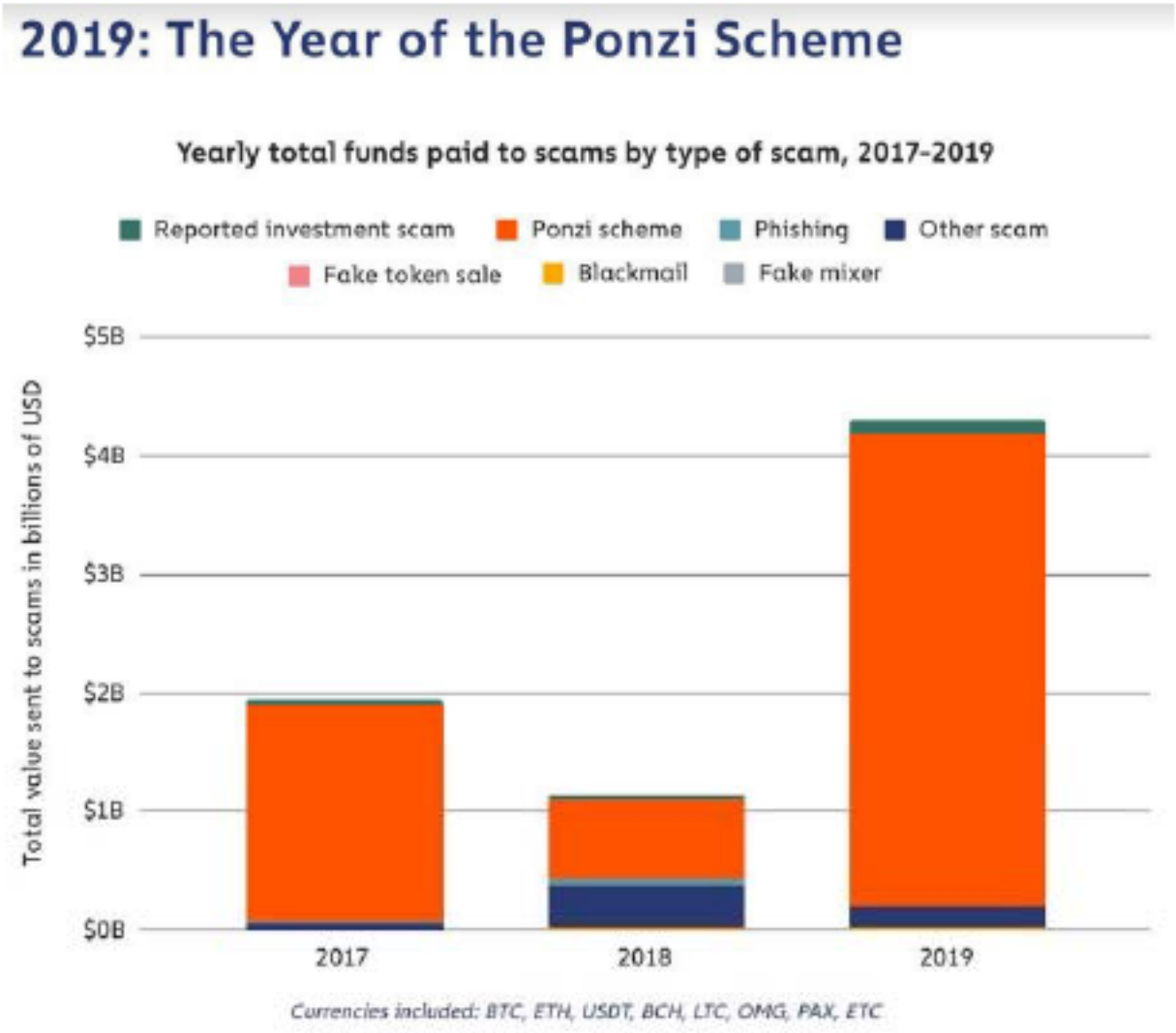


Figure 20 – Funds paid for Crypto Scams 2019

Source: https://www.chainalysis.com/

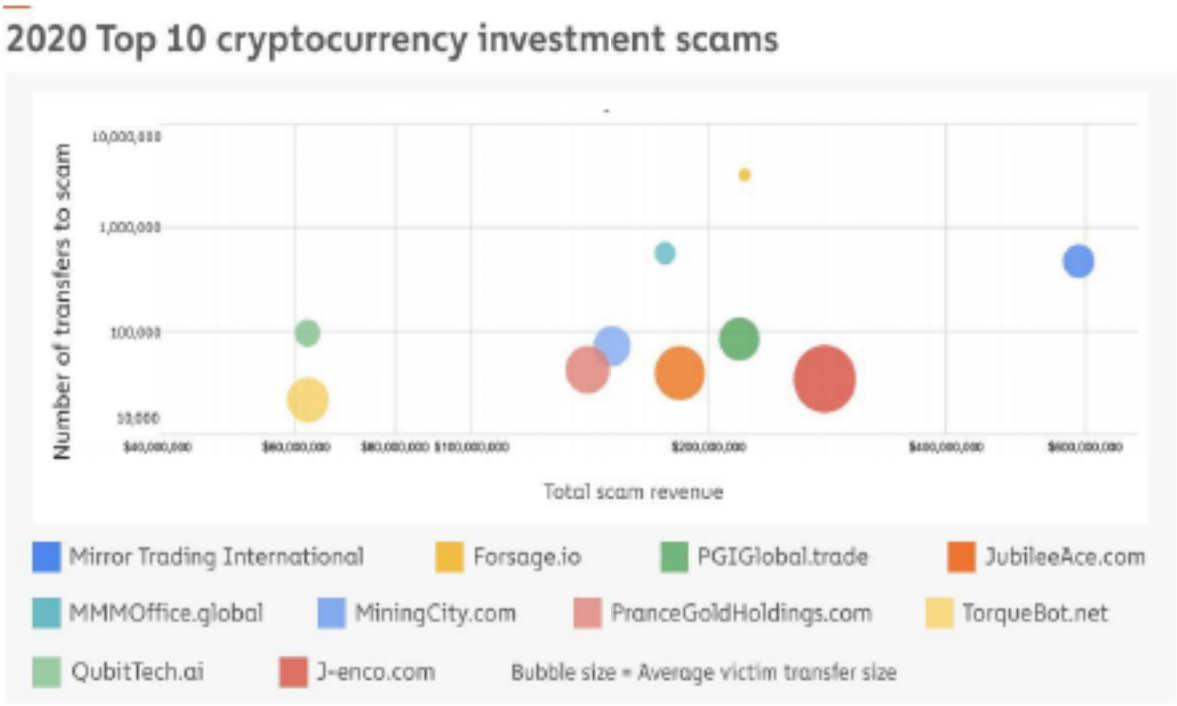


Figure 21 – Funds paid for Crypto Scams 2020

Source: https://www.chainalysis.com/

There are also many Ponzi schemes and pyramid schemes designed with the same goal of defrauding unsuspecting or naive investors.

Law enforcement officers should be alert to schemes where the novelty of cryptocurrency is used as a way to distract attention from the nature of the scheme.

E) Theft of Cryptocurrency

The theft of cryptocurrency is very common. Criminals can use malware or phishing to steal private keys. There have also been instances of very wealthy cryptocurrency users being kidnapped and forced to release their passwords to their kidnappers.

F) Cryptojacking

The world of Cyber Crime has seen several innovative means of attacking and exploiting infrastructure right from Cloud Computing resources to traditional Hardware devices such as Workstations, GPUs, and Desktops. To understand Cryptojacking, we need to first understand Cryptomining.

Cryptomining: The usage of computing resources such as CPU, GPU, or Cloud resources of an end-user or an industry to solve a mathematical puzzle (Proof of Work) to guess the right value before updating the ledger is known as Cryptomining. This allows hackers to be in a win-win situation as they have nothing to lose and the entire cost of wear and tear, electricity bills for the computing resources are borne by the victims.

Cryptojacking is a type of attack wherein hackers exploit vulnerabilities in the target's infrastructure to inject mining scripts to run on the target's Servers or Cloud resources without the knowledge of the owner. These scripts often supersede the legitimate purpose of the server or computing power rendering poor performance of the target system.

Browser Mining: Along with Cryptocurrency comes the term Browser mining wherein hackers exploit website vulnerabilities of a target and inject their mining scripts via a browser which in turn allows the script to be run on the Computing resource where the website is hosted.

The figure below illustrates the various symptoms to be noted to detect Cryptojacking.

Figure – 22 Symptoms to detect Cryptojacking

Source https://www.varonis.com/

7. SOP for the seizure of Cryptocurrency

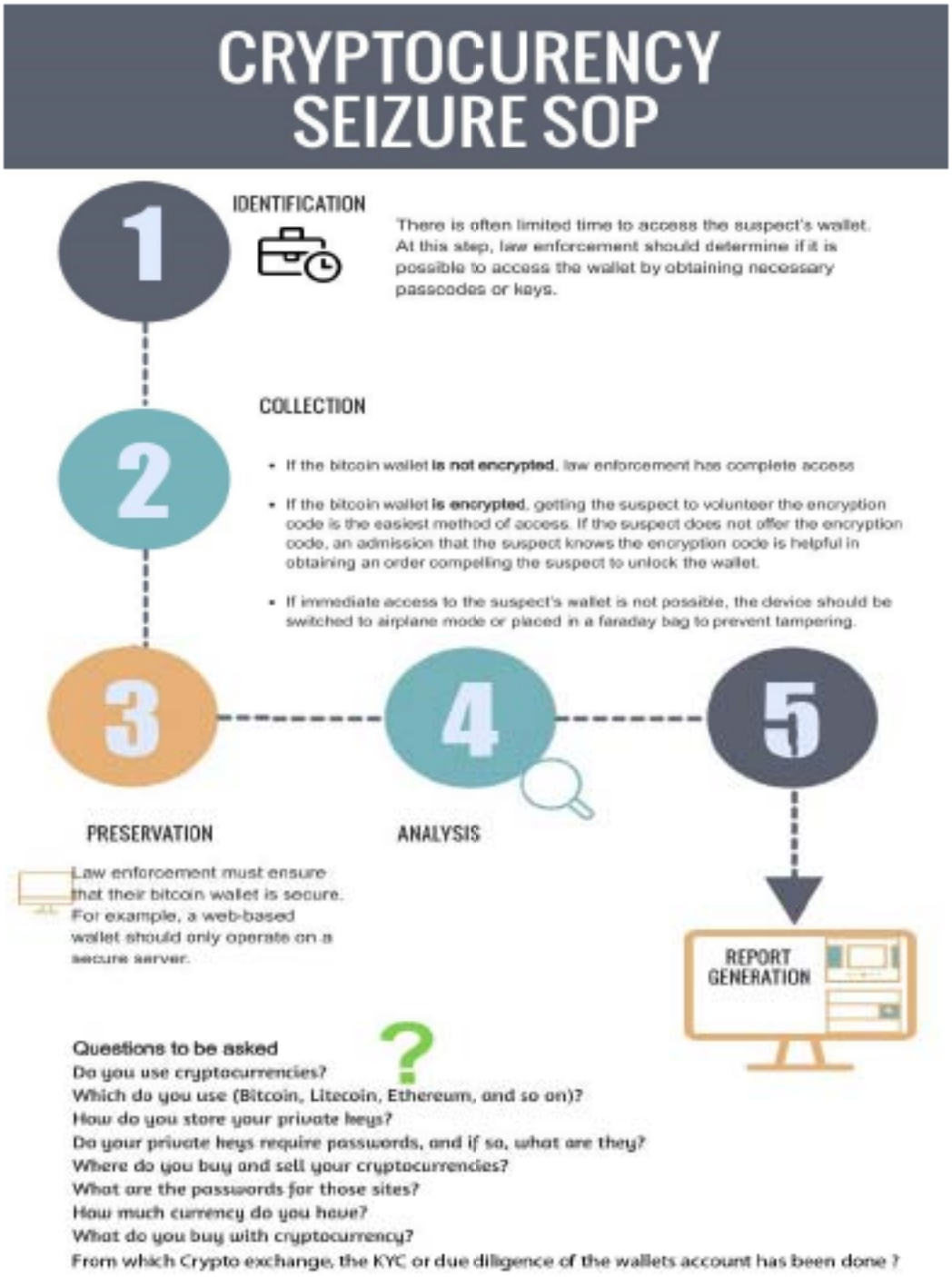


Figure 23 – Cryptocurrency Seizure SOP

How will the containment of network help in restraining the crypto currency? The wallets can also be accessed through web browsers and using paper keys. The seized currency is required to be transferred to official wallet or the respective exchange has to be directed to freeze the seized currency. In case of Private Centric wallets, the issuing exchange may be directed to freeze the transactions from the wallet

1) Identification – Once it has been established that there has been the involvement of bitcoins in a crime there should be a quick response by law enforcement agencies to seize bitcoins. At this step, law enforcement should determine if it is possible to access the wallet by obtaining the necessary passcodes or keys. the various types of wallets have been already covered in **Chapter 5** officers should be well versed with them so they can identify and prepare for seizure.

Access should be restricted to all devices that may contain bitcoin.

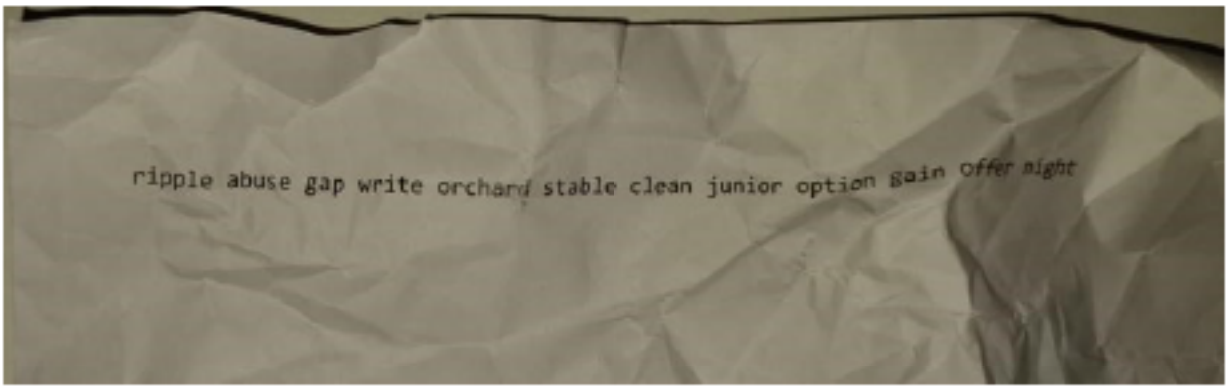


Figure – 24 Sample Seed password

The above fig is an example of a wallet seed password that can be used to recover a digital wallet[1] in case the password isn't available

2) Collection – Law enforcement agencies must have their own bitcoin/crypto wallet to store seized bitcoins/crypto The following scenarios are there.

1. If the bitcoin wallet is not encrypted, law enforcement has complete access (provided proper warrants have been obtained for the seizure of the device).

2. If the bitcoin wallet is encrypted, getting the suspect to give away the encryption code/ passwords/ seed words is the easiest method of access.

3. If immediate access to the suspect's wallet is not possible or the suspect is denying to provide password /encryption key, the device should be switched to airplane mode or placed in a faraday bag to prevent tampering (in case of a mobile phone)

If the wallet is a software

Note: Mobile phones must be later analyzed in signal jammer lab

1 Wallets are changing on a daily basis and security level is increasing we have taken into consideration the standard wallet in our SOP

Flowchart- Seizing Cryptocurrency (computer-based wallet)

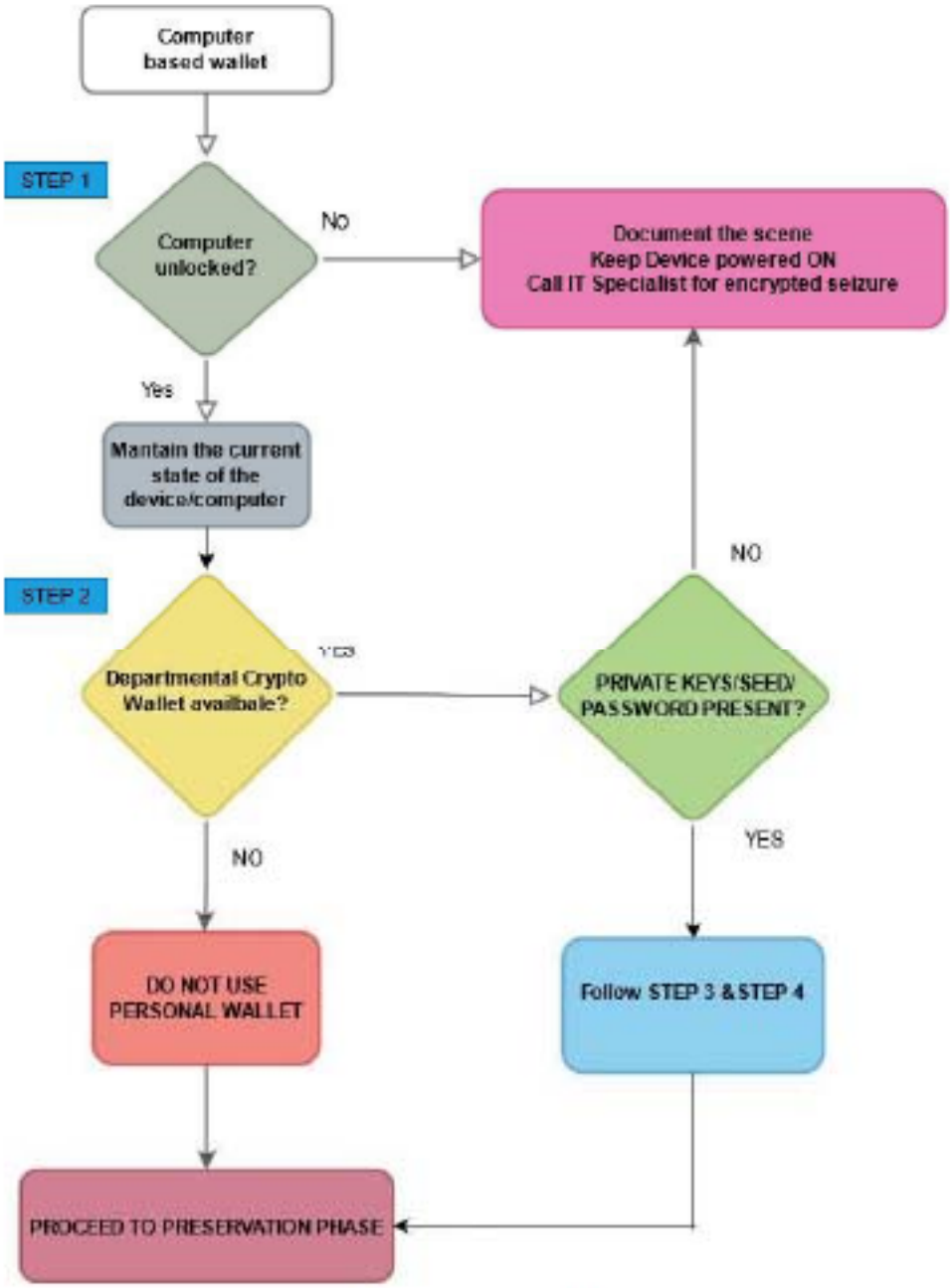


Figure – 25 Seizure for Compute based wallet

Note: For Acquiring Forensic image of Computer systems please refer to "Best Practices for First responders in context to computer systems -NCRIC (BPRD) "

Flowchart- Seizing Cryptocurrency (Mobile-based wallet)

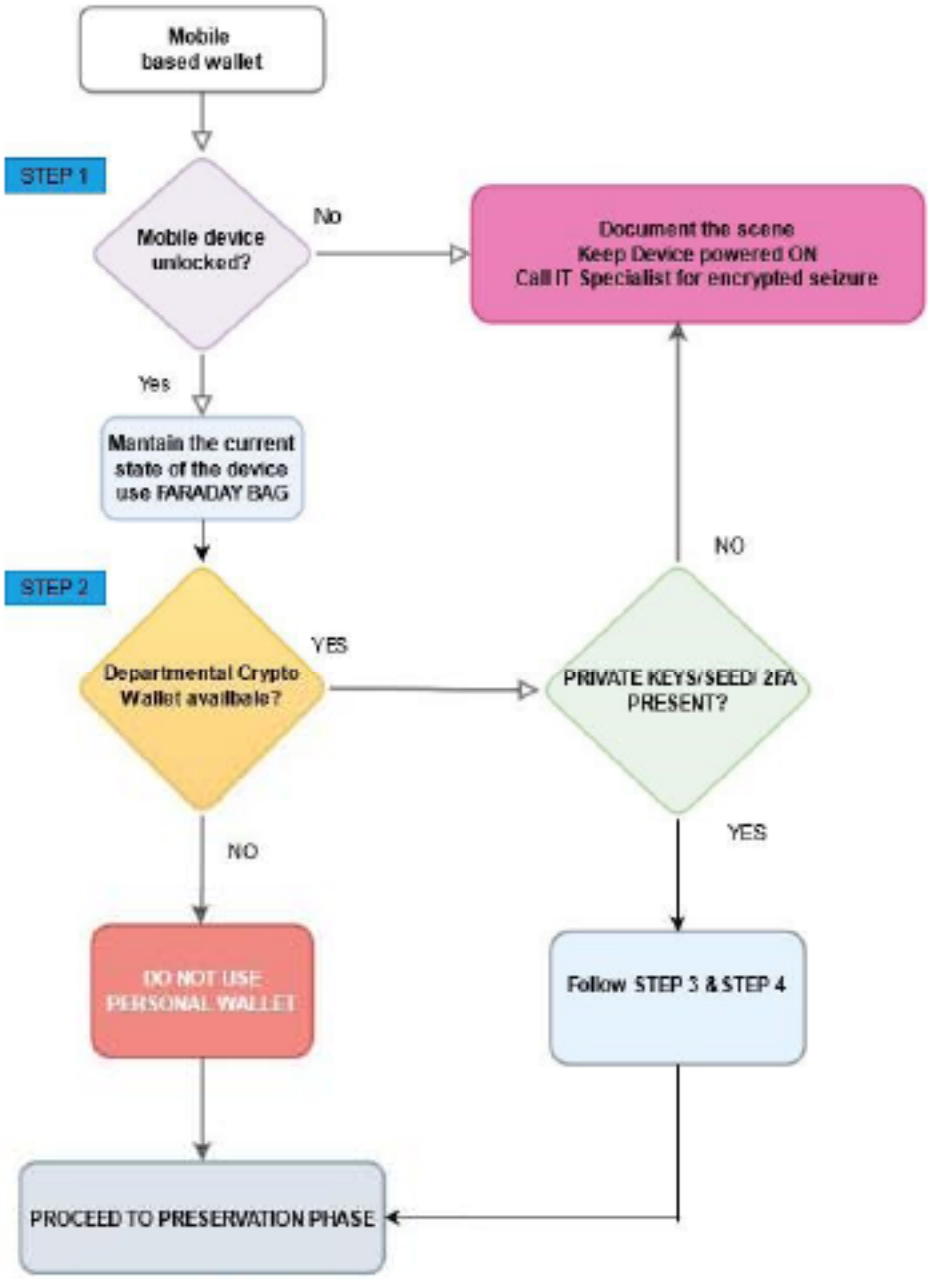


Figure – 26 Seizure of Mobile based wallets

Note: Just as a mobile phone is seized it should be kept in a faraday bag/ airplane mode to prevent remote tampering, as the mobile phone could contain seed words/ 2FA codes/private keys which are required to restore a wallet.

In case of seizure of any crypto currency the registered exchange (CX-Wallet Exchange) of the subject wallets may be liasioned for blocking the wallet or re-setting of the keys to defuse the transactions and if, the wallet belongs to DX (De-Centralized Exchange), then immediately transfer the currency into the departmental wallet. It is to be noted that the seized crypto currency may not be liquidated or converted into local currency; it may cause legal consequences to the department due to the fluctuation in rates of the crypto currency in the market.

Step 1 As in all cases involving evidence, responding personnel should thoroughly document the scene.

Figure – 27 Faraday Bag

Source:https://prosecman.com.au/product/mission-darkness-medium-neolok-faraday-bag-non-window-advanced-wireless-device-shielding/

When a Crypto wallet is discovered, access to it is often protected by encryption. In the event the suspect's computer or mobile device is unlocked, follow best practices for maintaining the current state of the device to prevent it from locking from inactivity. In the case of a mobile phone, a faraday bag should be used.

Step 2 Ensure the authorized person at the location has access to the crypto wallet. wallet. Without a crypto wallet please DO not use a personal wallet and proceed towards the preservation phase.

If a Departmental crypto wallet is available the officer needs to make sure he has the access to the suspects crypto wallet he has to look out for:

- Seed passwords
- Passwords

- Private keys
- 2FA codes

Figure – 27 Collection of evidence to look out for at a Crime Scene

Following scenarios are there

- If a crypto wallet is unlocked 2FA and password is not required only an OTP is required while doing the transfer
- If a crypto wallet is locked password is present 2FA is also available

The crypto-wallet can be opened in another device by documenting the whole process with an independent witness by following the proper chain of custody[2]

- If a Crypto wallet is locked and password/2FA is not available

There are still chances of obtaining the seed words which can be used in turn to restore the crypto wallet Forensic expert should be consulted with they can restore the seed words and wallet addresses from the *wallet.bat* file this process will be discussed in the chapter 8:Evidence of interest.

Step 3 Depending on the type of Bitcoin wallet encountered, follow the below process.

Wallets can be many types such as Mobile, software, hardware, cold paper exchange-based, etc. The steps to transfer/seize Cryptocurrency vary with each wallet type.

Mobile wallets: If the suspect is using a mobile wallet, the process for making a transfer is relatively simple.

Step1: In the suspect's wallet, navigate to the transfer/withdraw or send tab.

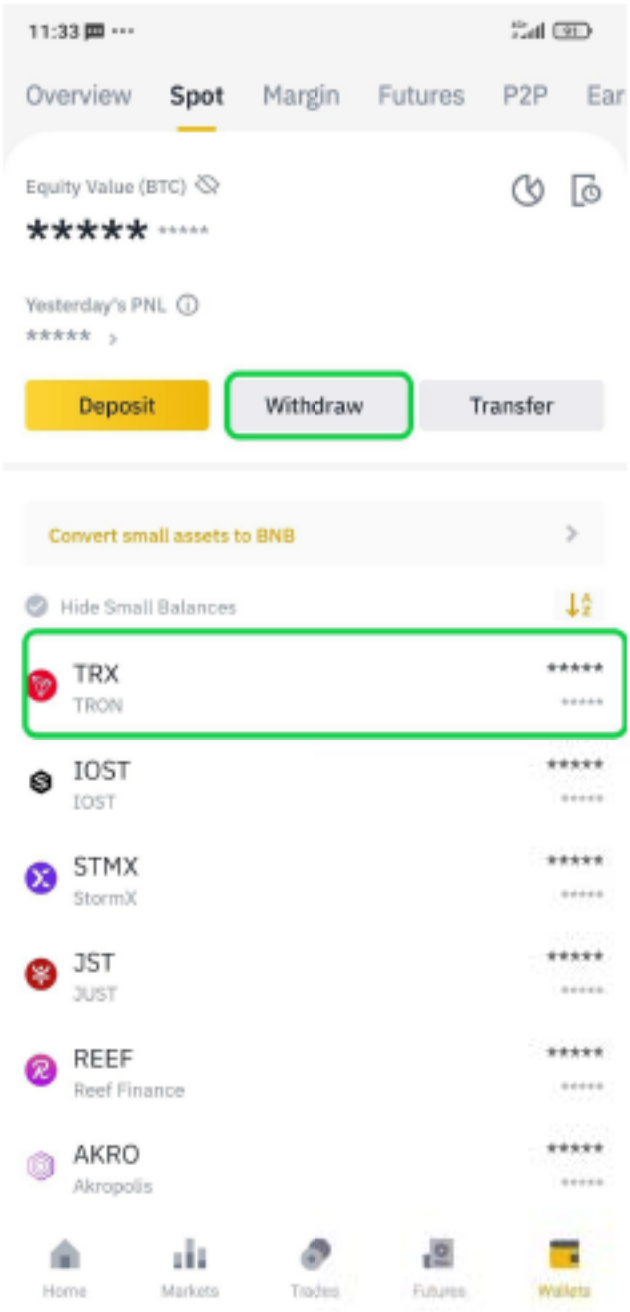


Figure – 28 User Interface of Binance Mobile Wallet

Step2: Enter the department wallet's address or scan its QR code in the space labelled recipient.

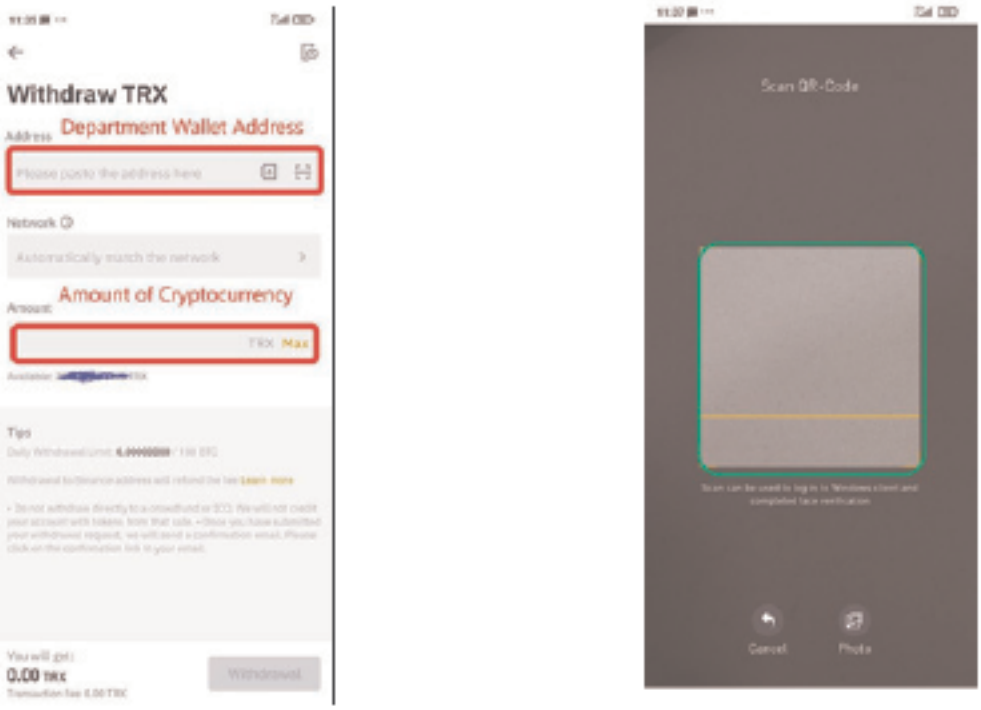


Figure – 29 User interface while transferring Crypto Currency (Binance)

Step3: Enter the full value of the wallet as the amount to be transferred.

Step4: Then press transfer or send to move the funds to the department wallet.

Note- while seizing mobile wallets it must be kept in mind that mobile wallets have 2-factor authentication methods. An OTP on mail and phone number is required for the transfer of funds

If the phone is unlocked

So the I/O team must ensure to collect

- A password of the wallet
- The 2FA codes which are present in the mobile phone

Software wallets: Generally, funds can be obtained from a software wallet using the same method as a mobile wallet.

However, with a software wallet, the suspect's private keys may be available either within the wallet or stored elsewhere on the device. Access to a suspect's private keys gives indefinite access to the accounts associated with those keys. While it is not recommended that the officer attempt to access the private keys, it is important that the device is treated as an encrypted device and seized, even if the officer can transfer the Bitcoins.

Following are the steps the LEAs must perform on any suspect's System while investigating

Cryptocurrency related crimes.

1) Connect a write blocker to the system and document the whole process

2) Enable the option to view hidden files and folders.

Control Panel > Appearance and Personalization. Select Folder Options, then select the View tab. Under Advanced settings, select Show hidden files, folders, and drives, and then select OK.

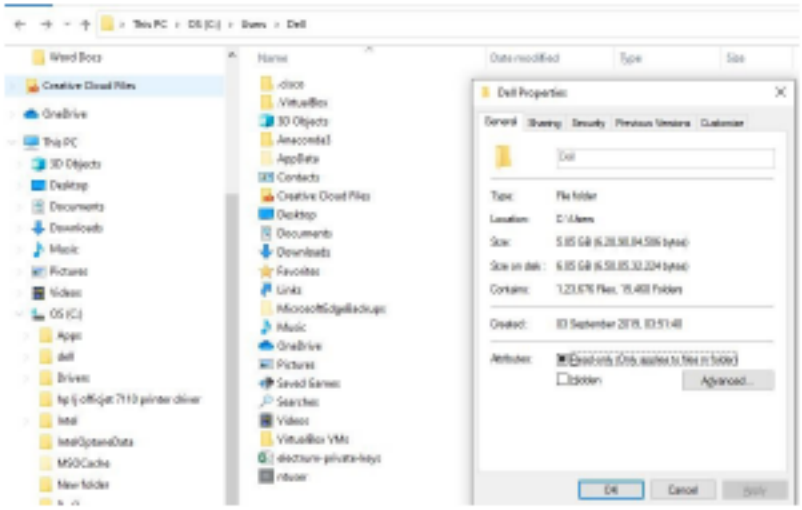


Figure – 30 Listing all hidden files

Step 2 – Browse the following folder to locate the 'AppData' folder. Look for the different online Cryptocurrency wallets. For example, the above image has been shown for Exodus.

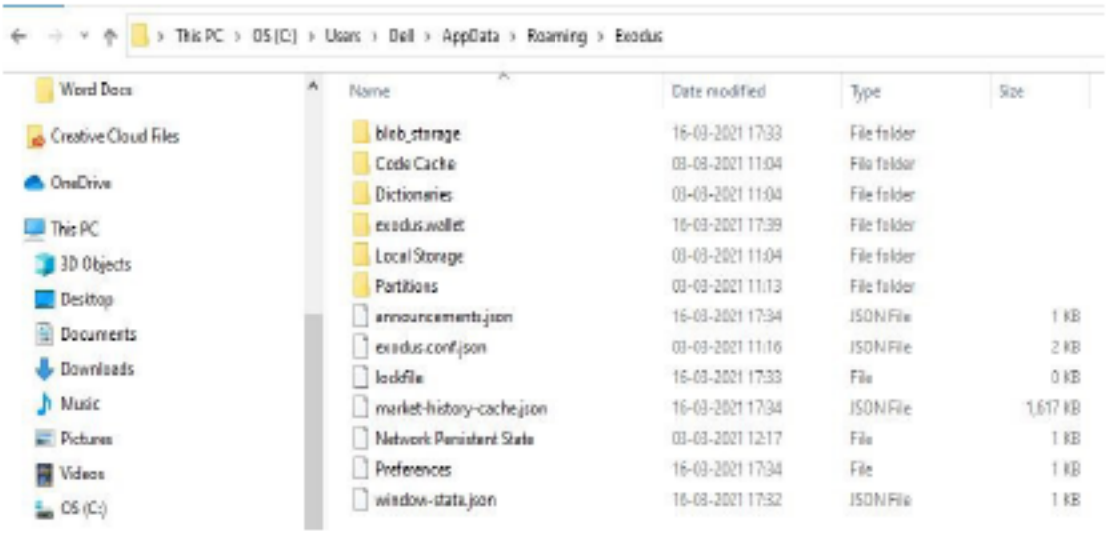


Figure – 31 Viewing files related to various Crypto wallets installed

Step 3 – After having confirmed, click on the shortcut icon of the wallet to open the wallet's user

interface.

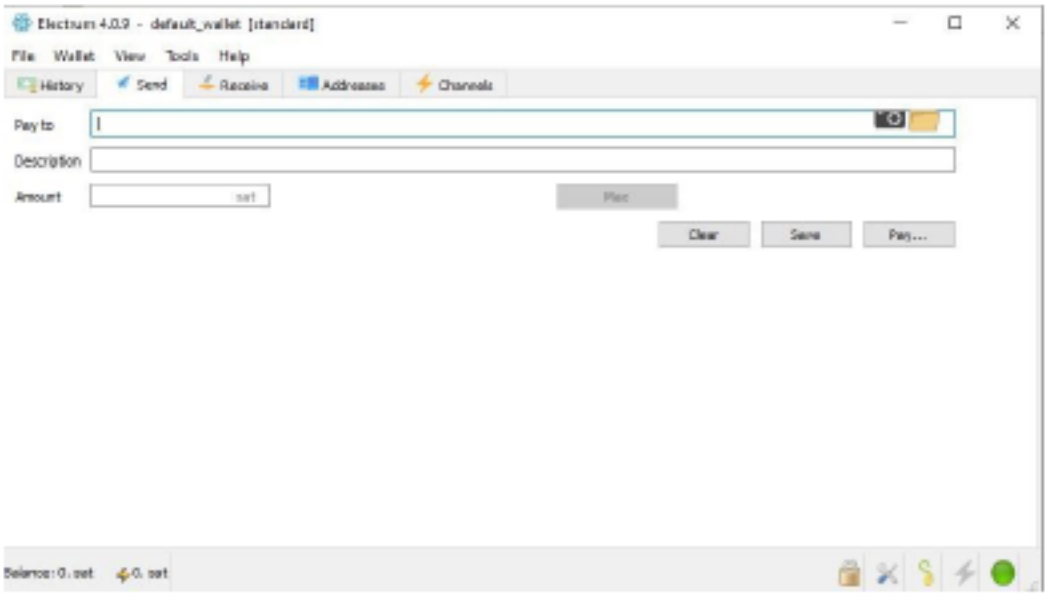


Figure – 32 Receipt address and details on Exodus User Interface

Step 4 – Either ask the suspect for any Passwords, seeds, or any credentials required to login into the Wallet. A good practice is to look around for any possible trashed papers for Seeds or any credentials as well.

Step 5- Once the wallet has opened in pay to section add the address of departmental wallet address

Online Wallets: If a suspect is using an online wallet, police can use the above method to transfer funds. Because online wallets use a third party to store Bitcoin funds, that third party can freeze accounts and assist in the seizure of funds left online. Police can do so using the same method to freeze traditional bank accounts, but the warrant must be directed at the online wallet operator.

Hardware wallets: Because hardware wallets are external memory or paper QR codes containing private keys, they must be loaded into a wallet that allows private keys to be imported. For an officer seizing the property of a suspect, it is sufficient to secure the hardware wallet and get it into the hands of an IT specialist as soon as possible.

If the suspect's phone/tablet/computer is present, the I/O team has to make sure to look for an app/ program called Ledger Live. This app connects with the hardware wallet where the private key is present.

NOTE: *It is important to remember that a wallet may have multiple files that are holding Bitcoin separately. If an officer is transferring funds from an open or unencrypted wallet, they should ensure that there are not multiple files in the wallet.*

8. Evidence of Interest

1) WALLET BAT FILE

This book is an introduction to cryptocurrency which deals with how to investigate and seize crypto crimes hence cryptocurrency forensics is not covered in this booklet, however

In some scenarios when the password is not available for a Desktop wallet, there are ways to restore a wallet using seed words. Seed words if not available can be recovered from the wallet backup file which is present in the computer.

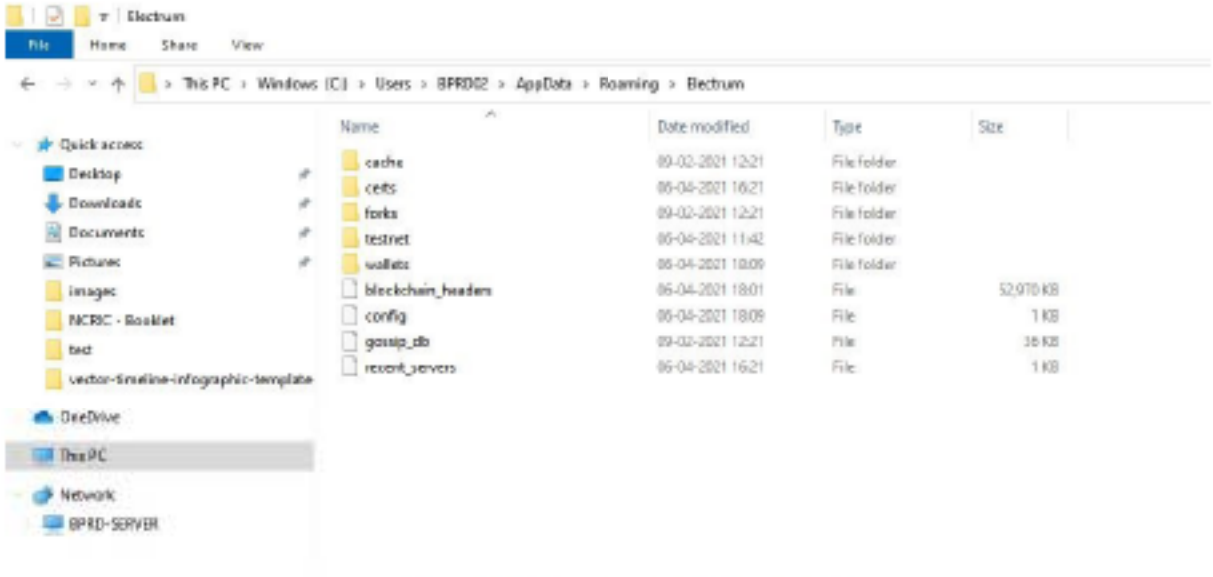


Figure – 33 Viewing the wallet ".bat" file

This folder can be accessed with a write blocker and the folder named wallets can be backed up to a destination drive which can be later used to analyze and extract evidence

In case a forensic image is already present it can be loaded in FTK imager and the wallet file can be copied to the destination drive

So this is an example of electrum wallet which is very popular

The location of the wallet file

C:\Users\BPRD02\AppData\Roaming\Electrum

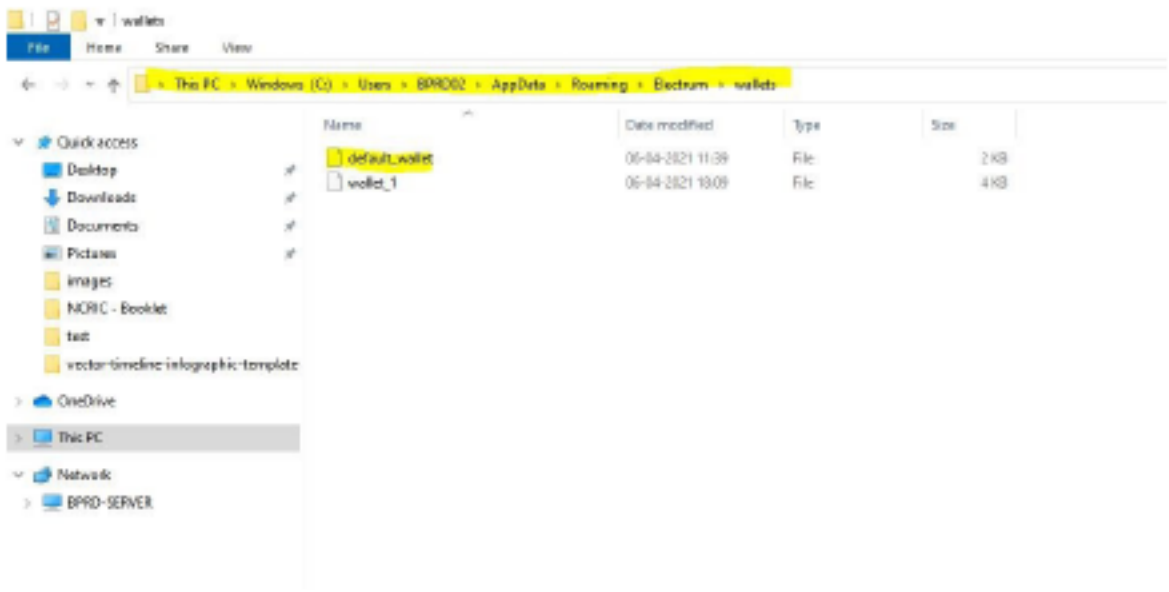


Figure – 34 Location of the .bat file from Crypto wallets (Electrum)

Once we have acquired the wallet.dat file which is highlighted in the above screenshot. We need to run it through Strings utility which can be found here https://docs.microsoft.com/en-us/sysinternals/downloads/strings

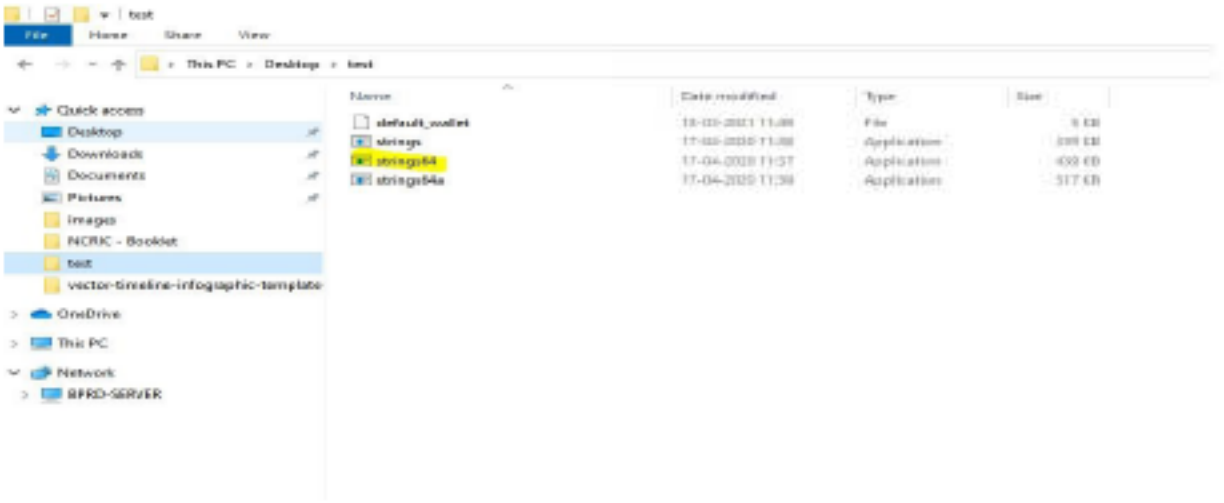


Figure – 35 Viewing the strings file

We need to extract it in a folder that also contains the wallet.dat file

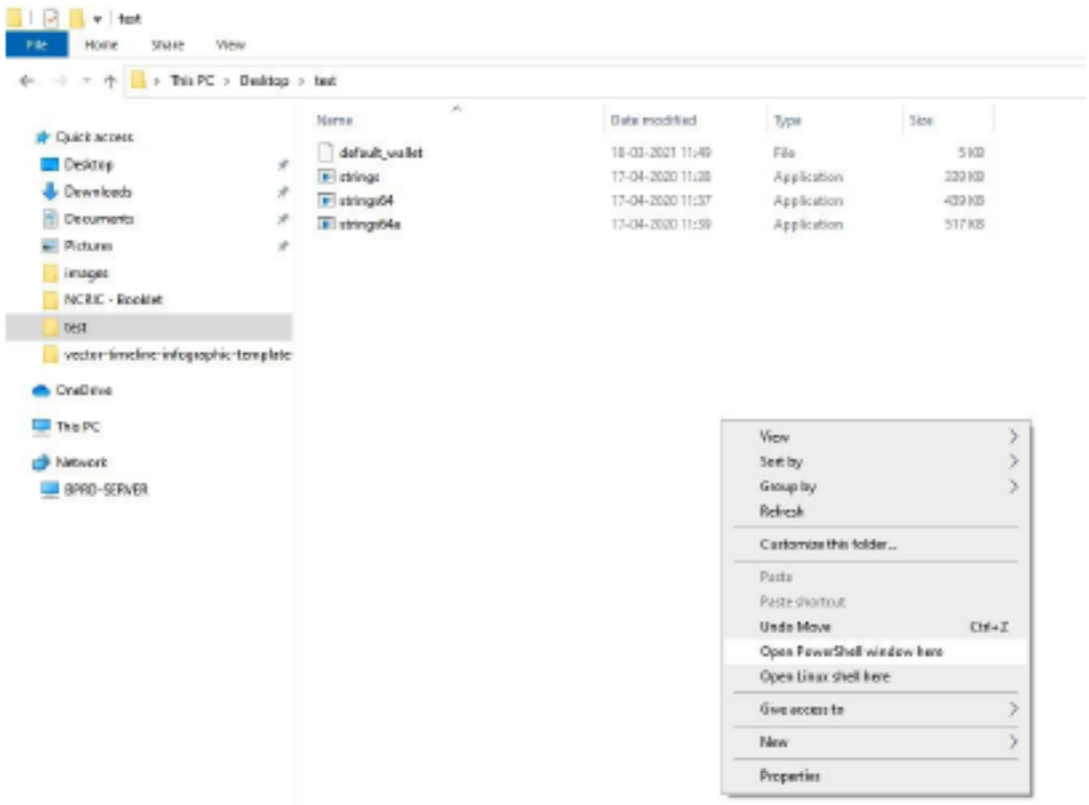


Figure – 36 Opening the Command Prompt

Click shift+right mouse click simultaneously to open the cmd/PowerShell prompt there and type the command as given in the screenshot below

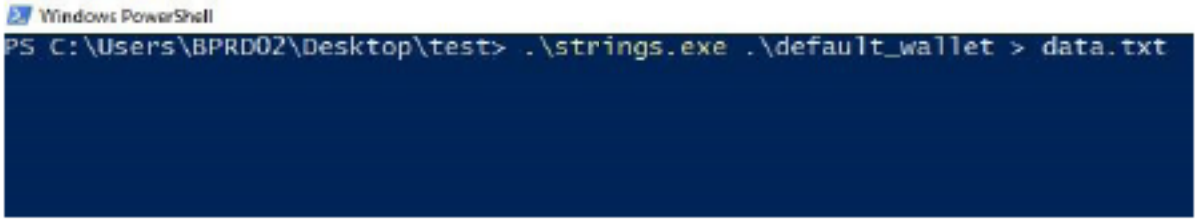


Figure – 37 Commands to convert .bat file contents to text

A file named data.txt will be formed in the folder after opening it has the following content The evidence of interest has been highlighted

The contents of the file data.txt are displayed below

Strings v2.53 - Search for ANSI and Unicode strings in binary images.

Sysinternals - www.sysinternals.com

"addr_history": {

"bc1q0290308uvlj4h2pfsp5kj4tgtrju644uulhnjl": [],

"bc1q08aspwvdtjc4kdeq35nyyy927r6775mz6jwqa4": [],

"bc1q0tykvv753c9f6puzlsmf7wktl3u9xwcavfz438": [],

"bc1q2ujhqdma4ahw3mc9158m8tsddnjgyxh7df3edj": [],

"bc1q2w6acwswt9mng331f88sp52vp44c9ffl2g84dc": [],

"bc1q40h02nl2r5x9cgacg6lmdft8jf447ncvnm9zlx": [],

"bc1q55jhvpx48w9r62y0z0chm0vy89m0djcw94j3zp": [],

"bc1q6veq9aphq4cg63qrl92ypysezr4g7qd34dfyqv": [],

"bc1q7pwp72kw8tejxru58nxz055gfz2hwe4mhqd49h": [],

"bc1q936v0r88e9rekscankasl9xjec3s7ax2axtvzk": [],

"bc1q99nh7sedq5xj3rrsswjsz5pzj7qf3qzu2g9ex3": [],

"bc1qcqmv2j35hsn0z6g5lc3kapex26288ds8dw6ev8": [],

"bc1qean5tpc4eztgpdwyt78tkl093uz5hnrs3fknl6d": [],

"bc1qejw2wmz6cx8gqr5vlwwy76m7pykqx9xa3anvej": [],

"bc1qekepz36y04hqy0p39nyvsekd24h7z27qc67vn3": [],

"bc1qfmsyw9pw29r9mdpxx3qa7vt8xsvx321q980535": [],

"bc1qgk6e6hwjp8uk3n4047sswr24u46dn7z8za8t7c": [],

"bc1qhh7jj9xqq6zuqwut3fnelk8cn9h9w2x83z5732": [],

"bc1qkdjdp4w9c9ngju50vgfjeadl0dmqevv9gce0kg": [],

"bc1qkx78019cds812relpwd2tdm2gdfevhxfnaa0fg": [],

"bc1qme28m885trrahkqecm9jyvr6vyh5lszq0qdwvj": [],

"bc1qmssu4n98eahlqvc4v3maem48uvsajrl5rw0vx2": [],

```
    "bc1qmyt3jrc4zlqma6vgn543ma3a4c98usqktvs3h9": [],
    "bc1qnz50hsja6ut9vlsca2xqkymker5fpncum8xk3w": [],
    "bc1qrw8axpxqgpfs6afg9c730c9rv0w3vwyxr2f347": [],
    "bc1qsj0vnm35thdxhgk22fjgqzqq8yzu35ze815gj7": [],
    "bc1qsw499ygjmgn8uums9adcgjtmtzlcw4h8wrl3rg": [],
    "bc1qsxj8pkm22qcsxldfj2d9xzl8knw02kkd7jj9pp": [],
    "bc1qv9r2r8p0pkfmy3s3xgdh4r5xhl2jtyj2sfzv0t": [],
    "bc1qvxjpmpvu0m3c73pk0e6ezxe9cz3qgctcckmegy": []
},
"addresses": {
    "change": [
        "bc1qkdjdp4w9c9ngju50vgfjeadl0dmqevv9gce0kg",
        "bc1qgk6e6hwjp8uk3n4047sswr24u46dn7z8za8t7c",
        "bc1qean5tpc4eztgpdwyt78tk093uz5hmrs3fkml6d",
        "bc1qsw499ygjmgn8uums9adcgjtmtzlcw4h8wrl3rg",
        "bc1q0tykvv753c9f6puzlsmf7wktl3u9xwcavfz438",
        "bc1qsxj8pkm22qcsxldfj2d9xzl8knw02kkd7jj9pp",
        "bc1q936v0r88e9rekscankasl9xjec3s7ax2axtvzk",
        "bc1qv9r2r8p0pkfmy3s3xgdh4r5xhl2jtyj2sfzv0t",
        "bc1qmssu4n98eahlqvc4v3maem48uvsajrl5rw0vx2",
        "bc1q2w6acwswt9mng33lf88sp52vp44c9ffl2g84dc"
    ],
    "receiving": [
        "bc1q99nh7sedq5xj3rrsswjsz5pzj7qf3qzu2g9ex3",
```

```
            "bc1q7pwp72kw8tejxru58nxz055gfz2hwe4nhqd49h",
            "bc1q55jhvpx48w9r62y0z0chm0vy89m0djcw94j3zp",
            "bc1qnz50hsja6ut9vlsca2xqkymker5fpncum8xk3w",
            "bc1qekepz36y04hqy0p39nyvsekd24h7z27qc67vn3",
            "bc1q0290308uvlj4h2pfsp5kj4tgtrju644uulhnjl",
            "bc1q6veq9aphq4cg63qrl92ypysezr4g7qd34dfyqv",
            "bc1qnyt3jrc4zlqma6vgn543ma3a4c98usqktvs3h9",
            "bc1qhh7jj9xqq6zuqwut3fnelk8cn9h9w2x83z5732",
            "bc1q2ujhqdma4ahw3mc9158m8tsddnjgyxh7df3edj",
            "bc1qkx780l9cds812relpwd2tdm2gdfevhxfnaa0fg",
            "bc1qsj0vnm35thdxhgk22fjgqzqq8yzu35ze815gj7",
            "bc1q08aspwvdtjc4kdeq35nyyy927r6775mz6jwqa4",
            "bc1qrw8axpxqgpfs6afg9c730c9rv0w3vwyxr2f347",
            "bc1qvxjpmpvu0m3c73pk0e6ezxe9cz3qgctcckneggy",
            "bc1qejw2wmz6cx8gqr5vlwwy76m7pykqx9xa3anvej",
            "bc1q40h02nl2r5x9cgacg6lmdft8jf447ncvnm9zlx",
            "bc1qcqmv2j35hsn0z6g5lc3kapex26288ds8dw6ev8",
            "bc1qfmsyw9pw29r9mdpxx3qa7vt8xsvx32lq980535",
            "bc1qme28m885trrahkqecm9jyvr6vyh5lszq0qdwvj"
        ]
    },
    "channel_backups": {},
    "channels": {},
    "fiat_value": {},
    "invoices": {},
    "keystore": {
        "derivation": "m/0'",
```

"pw_hash_version": 1,
"root_fingerprint": "7440b4c0",
"seed": "obey polar local high utility sugar rhythm refuse knee allow inside fit",
"type": "bip32",
"xprv": "zprvAZREW3TuaGdctMfEELAZfQC148XqvC35UaT3E9PZ4ZhwTpg
LnWET1EXy13CrXA8yF6GRoKEbmZWGXsH6m1S5Q59PMnc4ZHTgncxjMhASPtw",
"xpub": "zpub6nQauYzoQeBv6qjhLMha2Y8jcANLKekvqoNe2XoAcuEvLd1VL3YhZ2r
SrMySrcRtR3UxbPGjaNaGw7K3urBQQ7zosXAuHRYVHAYnHh8YnCf"
},
"labels": {},
"lightning_payments": {},
"lightning_preimages": {},
"lightning_privkey2": "xprv9s21ZrQH143K3prT6JMH7DdhRvqSrT2LuDaSXtAaBmrgdFkCes
REjqHsJNApwe8aBR6AAWsWrg61gTS3L1ybNFjE5ZEYSUUpW7G63xYANFX",
"payment_requests": {},
"prevouts_by_scripthash": {},
"qt-console-history": [],
"seed_type": "segwit",
"seed_version": 33,
"spent_outpoints": {},
"stored_height": 675127,
"submarine_swaps": {},
"transactions": {},
"tx_fees": {},
"txi": {},
"txo": {},
"use_encryption": false,

```
    "verified_tx3": {},
    "wallet_type": "standard",
    "winpos-qt": [
        610,
        355,
        840,
        447
    ]
]
```


Figure – 38 Contents of the Data.txt file

In the above text file, we can get to know that the portions highlighted in yellow are of interest to us, particularly the seed word is visible in plain text as we can see that wallet type is standard.

this means that while configuring the wallet standard security measures have been applied and there is no encryption in this.

By getting the seed in plain text it is possible to then restore the wallet and transfer the crypto to the departmental wallet.

NOTE:

- Paper wallets and/or private keys (encrypted or not) can be duplicated and stored in multiple locations. on their local computer, another in a document stored in the cloud, a printout of the same in a safe with a friend holding a further copy. With multiple copies of the same private keys.
- Another method is storing the private keys on a low-cost computer such as a Raspberry Pi or a cheap laptop which is then kept air-gapped from all networks.
- Alternatively, a Linux live/TAILS CD or USB can be used to boot into a known-safe environment, with the private keys kept on a separate, possibly encrypted, USB flash drive.

2) Blockchain Explorers

There are various blockchain explorers available which help in getting more details from a crypto address they have features to search by address or transaction ID.

Let us take an example of a recent Twitter hack which happened where twitter IDs were hacked of people like Elon musk, jazz Bezos, bill gates, Kanye west, and several other celebrities and big company CEOs these accounts were tweeting a similar message along with a BTC address which was a major crypto scam.

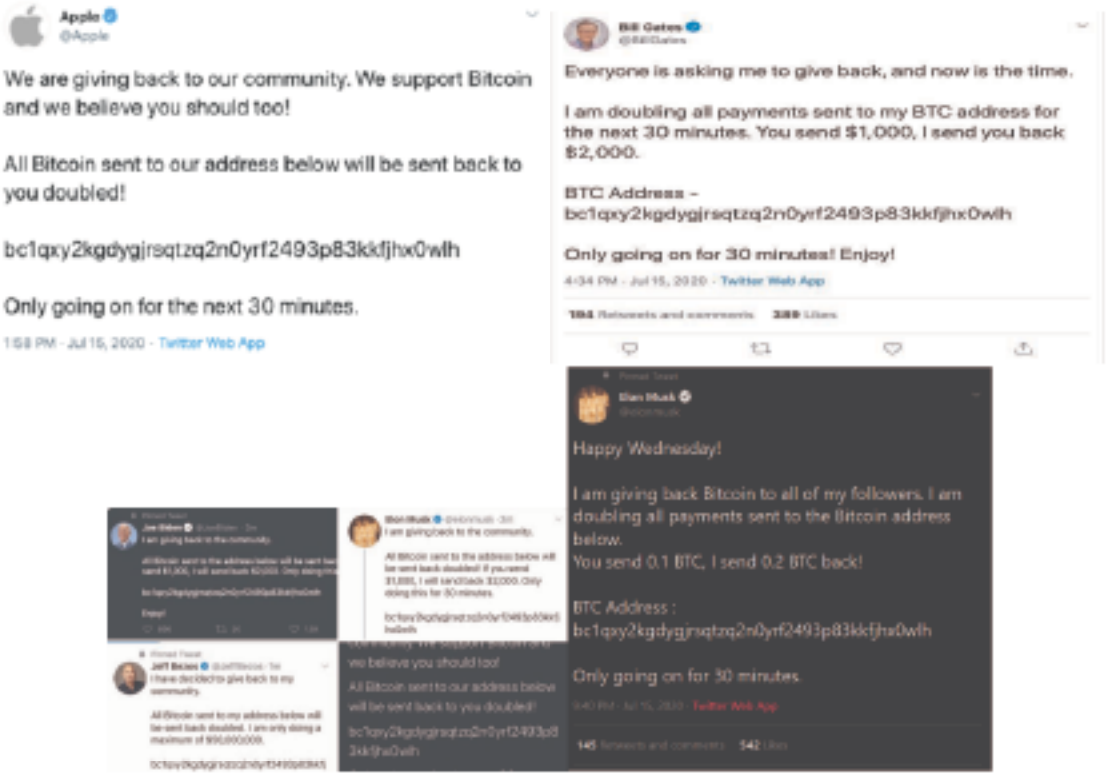


Figure – 39 Screenshots of tweets by Hacked Twitter Accounts

The bitcoin address is bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh

A Simple google search can get us many results let us use different types of blockchain explorers and see what information can be derived

A) Blockchain

Url: https://www.blockchain.com

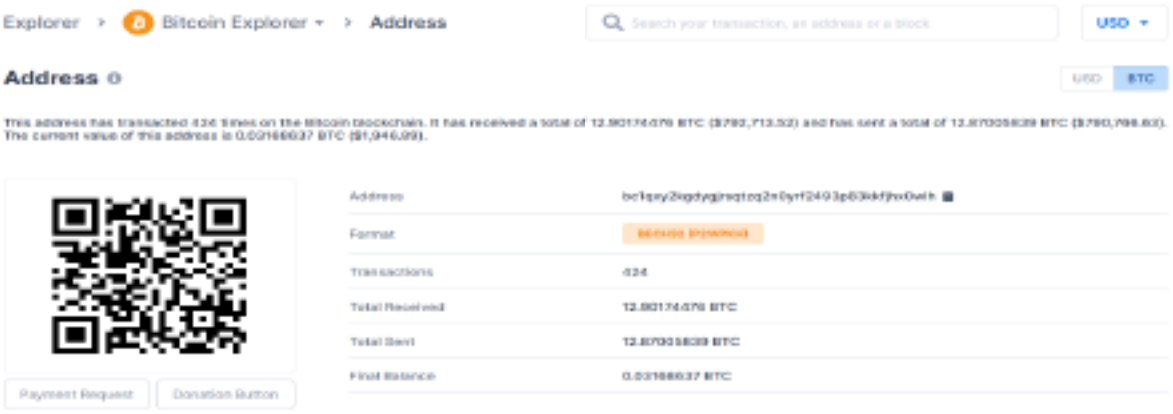


Figure – 40 Screenshot of Blockchain explorer

Figure – 41 Transaction Details

Transaction section

Hash: Called as transaction hash the green arrow shows that the left side-address

1pkq is transferring BTC to the right side bc1q address which is the scammer's wallet Address

We can see the date and time of the transaction and the miners fee is also there in the screenshot.

B) Oxt explorer

URL:https://oxt.me

Oxt Explorer is a good site to find the transaction details on a visual graph of first seen and last seen activities which are crucial in a piece of evidence.

It has various tabs such as the activity tab, temporal patterns, and Notes

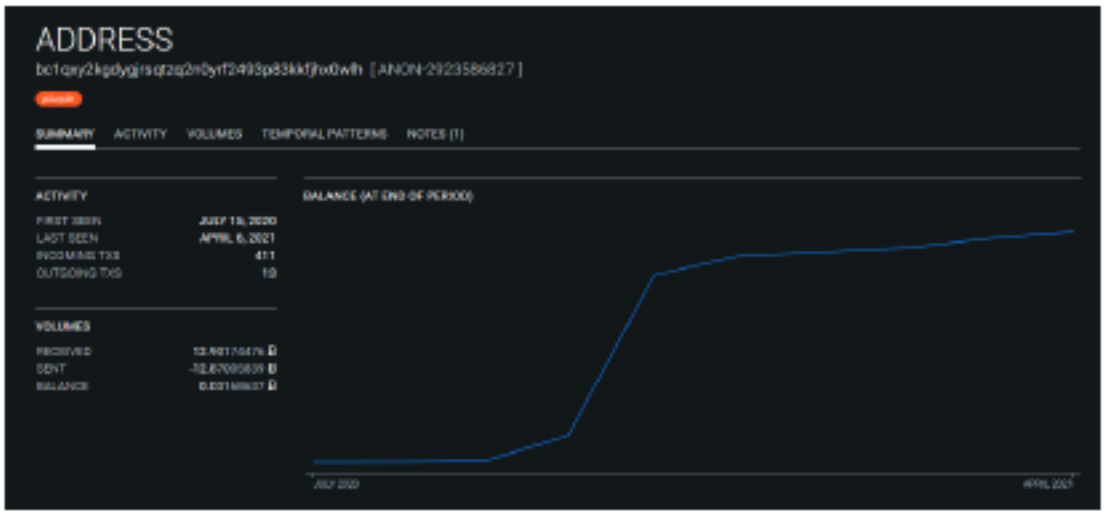


Figure – 42 Location of the .bat file from Crypto wallets (Electrum)

The temporal pattern helps in identifying the incoming and outgoing transactions for the address and which day of the week the wallet has been most active.

Figure – 43 Transaction patterns

Notes Section has the description of the address since it is crowdsourced this can be helpful for an investigator to get crucial information if its a popular wallet or a scam wallet related to ransomware ponzi scams etc

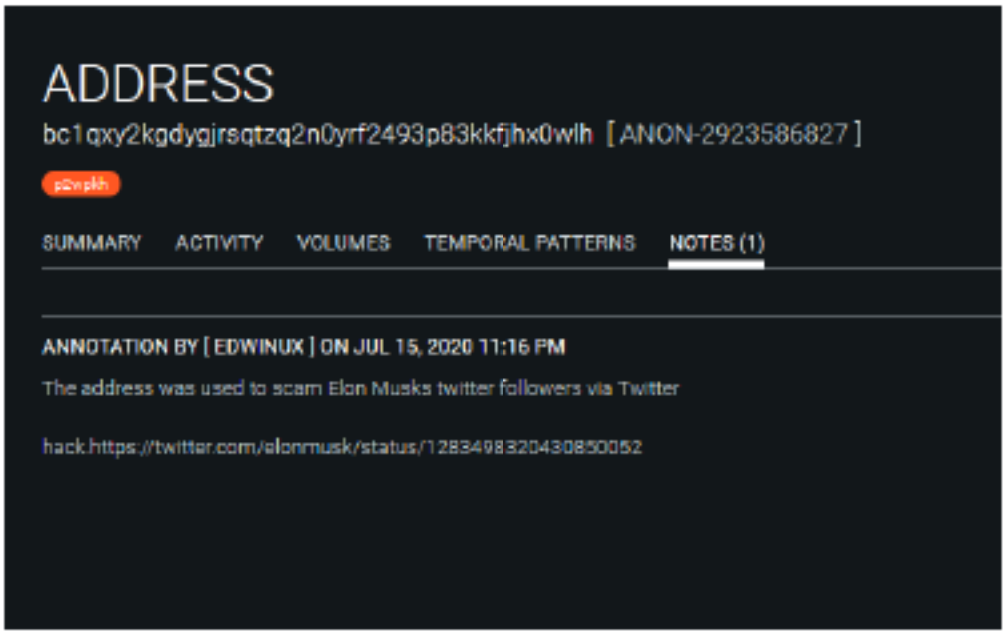


Figure – 44 Sample of wallet during Scams

Cross-referencing with https://www.bitcoinabuse.com/ we can get more information about the BTC address that its a scam address and many have reported against that address and links where the address has been featured.

Figure – 45 Bitcoin abuse database

Let us take an example of an individual wallet address 1Bm5ijTSELXBnZyiK5777fcWfArBR7teM4

A) Blockchain

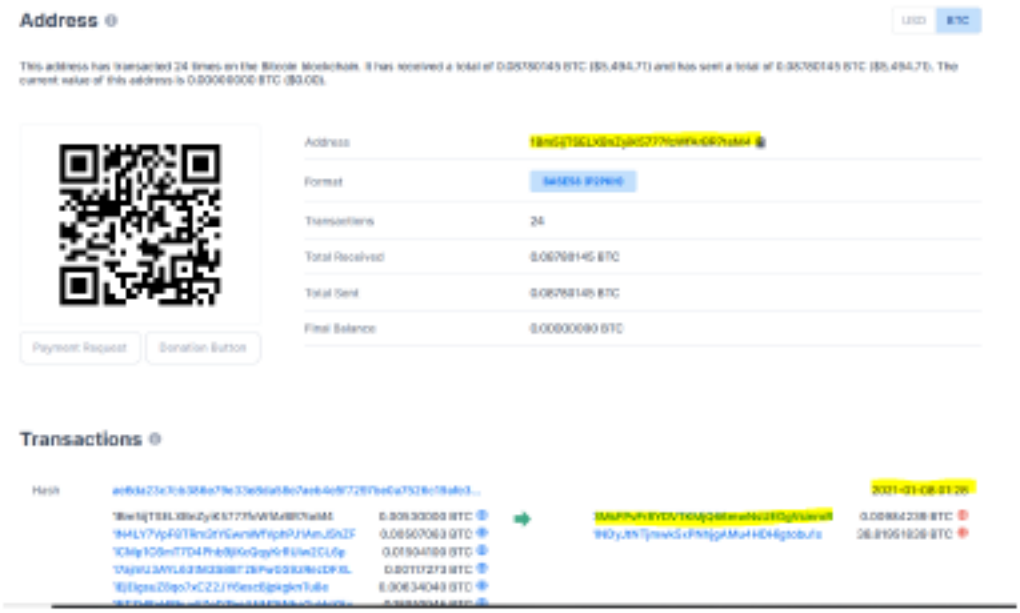


Figure – 46 Blockchain explorer

B) Oxt explorer

We can find out that this address belongs to Binance exchange

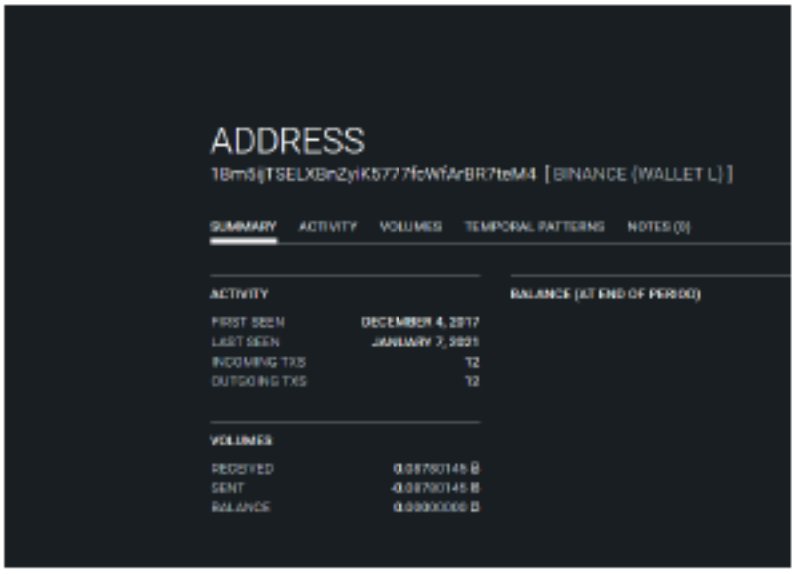


Figure – 47 Screenshot of OXT explorer

C) Blockchair

URL:https://blockchair.com/

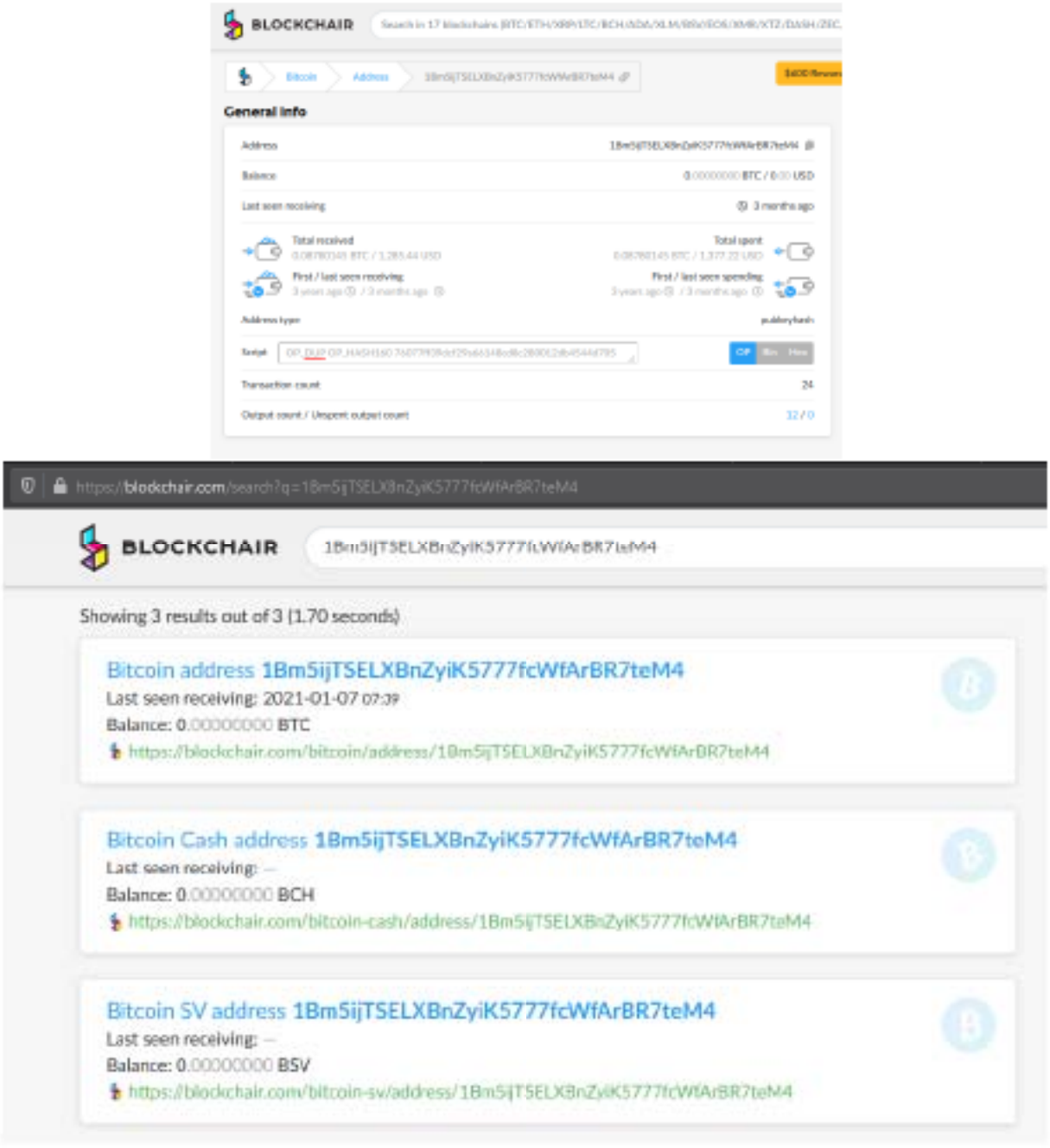


Figure – 48 User Interface of a Blockchair Website

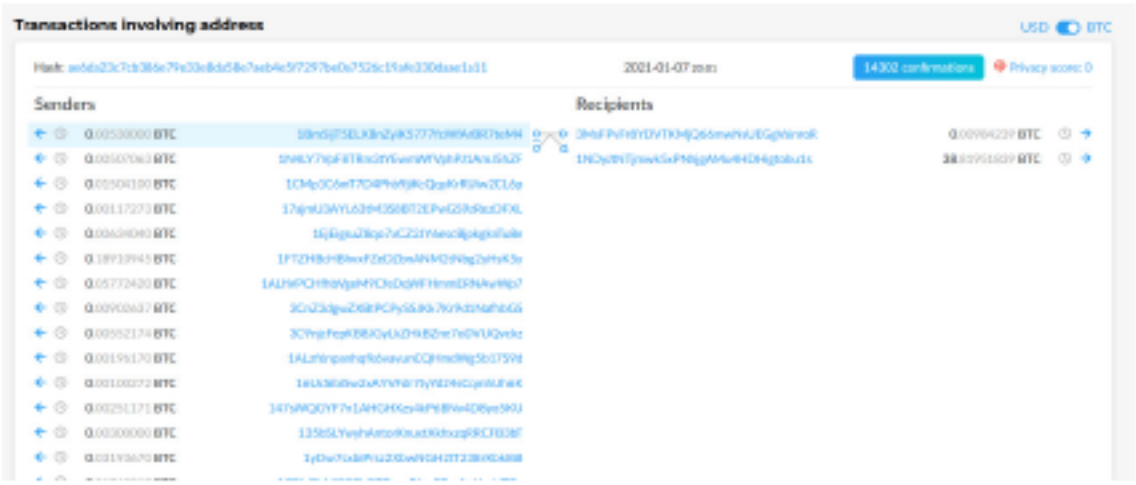


Figure – 48 Transaction shown in Blockchair website

The above explorers are fairly similar to each other and give similar results hence there is no need for further explanation. There is however a chance to get details of social media footprint IP address details of a wallet address in some cases as shown below

D) Bitcoin whoisWHO

URL: https://bitcoinwhoswho.com

This is a handy website to give us the social media footprint of the bitcoin address and also possible IP location (there are chances of the IP address being from a VPN or Tor network).

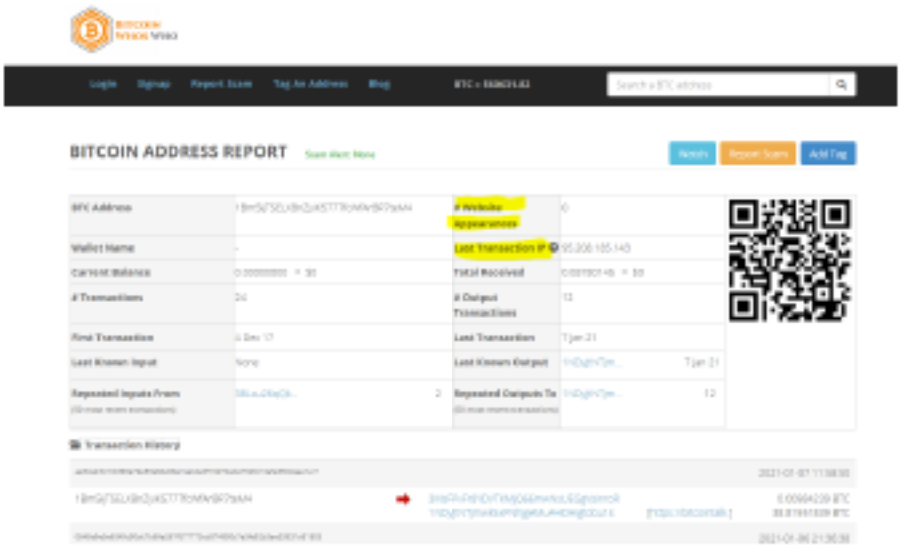


Figure – 49 Details of Wallet

There are quite a few advanced measures to trace the blockchain and map it on a graph format for tracking transaction node to node those methods are not in the scope of this introductory booklet

Chain analysis, cyphertrace, elliptical have commercial products to achieve the same

There is a simple method of tracking each transaction and plotting it on a piece of paper using

https://www.walletexplorer.com the author of which is presently working in the chain analysis team.

Figure – 50 Wallet Explorer transaction details

Samples of Crypto Addresses

Ethereum ETH or any ERC20 Token	0x68A99f89E475a078645f4BAC491360aFe255Dff1
BTC	bc1q220k2449fau0pxu9hfn28q3w4k99ep9hwsa5fa
DOGE	D6fWVp613N3dyLM6Zoghj3dZaEjbGZ8gpX
Tron or any TRC20 Token	TSZMcrQzMLdKrgiMPoe2uQMHLeEpkf2j8E
Cosmos	cosmos1sjrfyxwsvsslt4nzwqm0t6shghvylndxzf9tye
Tezos	tz1dMYz5pcXYXnfH5gjr652iSDq9zc2SrqRi
Solana	Gc6jm5gJVWE5DnjMMgzijghKYQqLTci9hZs7LYHYJs1g
Binance Smart Chain	0x5C9E5571B17D91e6ACcD4F0c29bBe199Af1f7B09
Litecoin	ltc1qcju52q8c3vv2a3uddx9zcna2sfg2mal84pa67z
Ripple (XRP)	rMX7JTCwp92WX1nyZsL3F8Hgc6ej8Q5Mud
Tron (TRX)	TDvt5uA9UBdvWJWvbSg2SqZ3MXSsLmA3oK

9. Law Related to Cryptocurrencies

RBI (Reserve Bank of India) has issued a circular on 6th April 2018 which states as follows

Technological Innovations, including those underlying virtual currencies, have the potential to improve the efficiency and inclusiveness of the financial system. However Virtual Currencies (VCs), also variously referred to as cryptocurrencies and crypto assets, raise concerns of consumer protection, market integrity, and money laundering, among others.

Reserve Bank has repeatedly cautioned users, holders, and traders of virtual currencies, including bitcoins, regarding various risks associated with dealing with such virtual currencies. Because of the associated risks, it has been decided that, with immediate effect, entities regulated by RBI shall not deal with or provide services to any individual or business entities dealing with or settling VCs. Regulated entities that already provide such services shall exit the relationship within a specified time. A circular in this regard is being issued separately.

10. Challenges Ahead

With ever changes in technology security has become more robust and cryptocurrencies are also improving their structure and hence it becomes difficult to seize them without having good knowledge of their architecture. The criminals are also employing new methods so that tracking them will become difficult for LEAs.

Multiple wallet addresses

Adversaries have got to know the pseudo-anonymous nature of BTC and have realized that they can be tracked they have resorted to using Monero and other privacy-centric coins. They have further complicated the tracking process by using a new wallet address for each new transaction this pattern can be found in any of the blockchain explorers, but makes it that difficult to trace them.

Bitcoin mixer service

Is a cryptocurrency service that allows users to "anonymize" their Bitcoins by eliminating any possible connection between their original deposited Bitcoins and the mixed Bitcoins that they withdraw later from the service This mixing process can make the tracking of Bitcoin movements between addresses challenging.

References

1. www.nw3c.org
2. www.imolin.org
3. www.iacpcybercentr.org
4. www.Ngm.com.au
5. https://thenextweb.com/hardfork/2019/12/26/bitcoin-cryptocurrency-criminals-l aw-enforcement/
6. https://www.police1.com/police-products/investigation/articles/what-cops-need-to-know-about-cryptocurrency-yt8aZISWOQKLqlc3/
7. https://www.interpol.int/en/How-we-work/Innovation/Darknet-and-Cryptocurre ncies
8. https://blog.malwarebytes.com/opinion/2020/03/are-our-police-forces-equipped-to-deal-with-modern cybercrimes/

officialBPRDIndia

BPRDIndia

Bureau of Police Research & Development India

bprdIndia

www.bprd.nic.in

Cyberdost

www.cybercrime.gov.in

NATIONAL CYBER CRIME RESEARCH & INNOVATION CENTRE (NCR&IC)

BUREAU OF POLICE RESEARCH AND DEVELOPMENT

Ministry of Home Affairs, Government of India

NH-8, Mahipalpur, New Delhi-110037