ISSN 2583-8504
Vol-2 (No.1) • December 2023

NCRB

आज़ादी का अमृत महोत्सव

NCRB JOURNAL

www.ncrb.gov.in

National Crime Records Bureau

New Delhi

RNI NO. DELENG/2022/83753

NCRB JOURNAL

Vol-2 (No.1) • December 2023

Published by National Crime Records Bureau, Ministry of Home Affairs, Government of India, National Highway-48, Mahipalpur, New Delhi – 110037.

Printed by Smat Forms, 3588, G.T. Road, Old Subzi Mandi, Delhi-110007

NCRB JOURNAL

Vol-2 (No.1) • December 2023

BOARD OF REFEREES

NCRB JOURNAL

Vol-2 (No.1), December 2023

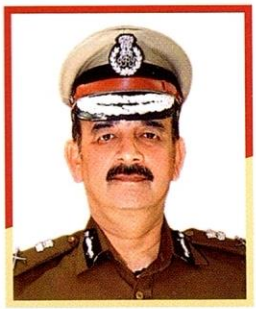
Contents

EDITORIAL BOARD

About Us

The inaugural issue of the NCRB Journal was released in 2022 by National Crime Records Bureau (NCRB). It is an annual English publication that features articles on police related subjects like police science, law, scientific investigation, criminology, forensic science, fingerprint science, physical / biological / behavioral measurements, biometric science, contemporary legal issues, cyber-crime, cyber terrorism, cyber security, socio-economic crime, prisons, etc.

The contributors to its articles include senior police officers and scholars from various prestigious institutions across the country. The articles are reviewed by a Board of Referees before being published. It is distributed free of cost to various dignitaries of Ministry of Home Affairs (MHA) and higher officers of States/UTs viz. Chief Secretaries, DGPs, Heads of CPOs, SCRB heads, Police Training Colleges etc.



EDITORIAL

It gives me immense pleasure in bringing out the second issue of NCRB Journal. This is a peer-reviewed and multi-disciplinary journal with well-researched articles on topics such as Police Science, Criminology, Forensic Science, Contemporary Legal Issues, Cybercrimes etc. The articles cover a diverse spectrum, each by shedding light on key advancements in technology and use of scientific techniques such as Fingerprint Science, Blockchain Technology, in combating crime.

In the article "Identification and Extraction of Crypto Currency Artifacts AI/ ML-Toolkit for Investigators/Forensic Examiners", the author underscores various dimensions of Blockchain and cryptocurrency, an evolving form of financial crimes due to their inherent anonymity. Over the past 15 years, the proliferation of virtual assets has spurred digital forensics research on crypto wallets. This study introduces a tool with AI/ML algorithms to assist crime investigators and anti-money laundering efforts.

In the article "Open-AI Powered Powerful New Technology: ChatGPT & its Use(s) in Law Enforcement.", the authors present legal and technical recommendations aimed at regulating the use of ChatGPT and mitigating the potential for crimes associated with its utilization.

In the article "Study of Blockchain Forensics and Crypto currency Crimes in India Scenario", the author explores blockchain and cryptocurrency crimes in the Indian context, covering blockchain basics, forensics procedures, analysis tools, and the utilization of blockchain in Indian law enforcement.

The article "Cyber Fraud: The Growing Cyber Crime", addresses the escalating issue of cyber crimes in India, emphasizing the prevalence of cyber fraud, its types, statistics over the past five years, and government initiatives along with preventive measures.

The article "Cyber Threat Intelligence: Current Status and Future Directions", underscores the escalating frequency of cyber-attacks, and delves into the critical role of Cyber Threat Intelligence (CTI) in fortifying organizations against evolving cyber threats, exploring its lifecycle, types, benefits, drawbacks, and future prospects.

In the article "Forensic Biometrics: A Revolutionary Approach to Reduce Crime", the author highlights the potency of Forensic Biometrics, particularly the Criminal Procedure Identification System in India, utilizing four unique biometrics to accurately identify habitual criminals and contribute to reducing recidivism, preventing crime, and expediting justice.

The article "The Art of Detection: Household Ingredients for Latent Fingerprint Development.", explores the field of dermatoglyphics, emphasizing the development of latent fingerprints on various surfaces using easily available non-toxic formulations and natural powders, with subsequent recording, lifting, and comparative analysis.

In the article "Identifying the Common Modus Operandi of Counterfeiting Syndicates Involving Identity Theft: Exploring Operation Cookie Monster", the authors delve into the global shift of crime, particularly counterfeiting, to cyberspace, focusing on "Operation Cookie Monster," a multi-country investigation targeting identity theft and counterfeiters, emphasizing the rising financial impact of cybercrime and advocating for enhanced collaboration between law enforcement and the private sector.

In the article "Solving Crime by Tracing Unknown Criminals through Scene of Crime Prints: A Short Review.", the authors underscore the enduring significance of fingerprints, particularly Scene of Crime (SoC) prints, for personal identification, revealing variations among states in tracing criminals until the implementation of NAFIS, emphasizing the importance of interconnected and effective databases for successful identification.

The last article "Blockchain Applications for Law Enforcement Agencies.", advocates for the adoption of Blockchain in law enforcement to enhance data storage security, efficiency, and transparency, presenting it as a superior alternative to traditional methods, particularly for storing public complaints, FIRs, trial details, and crime-related data.

I thank all the esteemed authors, who have sent their papers for this issue of the Journal. I also thank all the distinguished members of the Board of Referees for their valuable advice. I am sure that readers will find these articles thought-provoking and encourage them to further contemplate the relevant issues.

Vivek Gogia

(Vivek Gogia)

Identification and Extraction of Crypto Currency Artifacts AI/ML-Toolkit for Investigators | Forensic Examiners

Pravin Mandloi*

ABSTRACT

The terms "BLOCKCHAIN", "BITCOIN," "CRYPTOASSETS," and "VIRTUAL CURRENCIES" have all emerged to describe cutting-edge technology that quickly transfers value across borders. Blockchain and distributed ledger technologies, which are rapidly developing, have the potential to fundamentally alter the financial environment. Yet, individuals looking to avoid government inspection are also drawn to them because of their speed, worldwide reach, and – most importantly – anonymity. Almost fifteen years ago, the first blockchain was created. Since then, virtual assets have grown in popularity and have begun to be used as payment methods. *[1]*

Following this point, there was an explosion that gave rise to thousands of other cryptocurrencies and created a brand-new area of study for digital forensics investigators. The digital forensics of crypto wallets is the topic of this research. This paper intends to offer ideas and existing work on Crypto wallets and to target applications running on any operating systems (Desktop OS (Mac/Windows/Linux), Mobile OS (IOs, Android etc.)). The objective also included creating a tool for locating various artifacts that Crypto wallets leave behind on mobile and computer systems. At this time preliminary tool has been successfully created with the present AI/ML algorithms and can be used by Crime Investigators, Digital forensics examiners and Anti Money Laundering Investigators.

Introduction

Crime Investigations involving digital currencies, or cryptocurrencies, have become more prominent today. Every transaction involving cryptocurrency is preserved on the blockchain and is immutable in nature which ultimately helps fraud-related investigations. Bitcoin and other digital currencies offer more privacy than regular transactions. Instead of using personal information, they use cryptographic keys to show ownership. This makes them appealing to people involved in illegal activities. People can use them for corruption, money laundering, and avoiding taxes.

Author's Introduction:

* M. TECH | DATA SCIENCE, Superintendent of Police, Central Bureau of Investigation, New Delhi, INDIA

Bitcoin has been widely used to buy illegal things and services on NFT/Darknet markets.

Here are some reasons why investigating cryptocurrency-related crimes is essential:

Anonymity: Cryptocurrencies offer users a high level of anonymity, making it challenging for law enforcement agencies to track down criminal activities. When people use cryptocurrencies, their transactions get written on a public record, but figuring out who they really are in the real world is tricky. Checking these transactions can give important hints, helping the police find and catch criminals.*[2]*

Cross-border transactions: Cryptocurrencies are like digital money that can move between countries without using regular banks. This makes it hard for cops to follow the money and catch people doing bad things globally. Checking cryptocurrency transactions can help find and stop these illegal activities. *[2]*

Cybercrime: Cryptocurrencies are frequently used to pay for ransomware attacks, hacking services, and other cybercrime activities. Investigating cryptocurrency transactions can help law enforcement agencies to identify the perpetrators of cybercrime and prevent further attacks.*[2]*

Money laundering: Criminals often use cryptocurrencies to launder money by converting their illegal proceeds into cryptocurrencies and then back into traditional currencies. Investigating cryptocurrency transactions can help to identify the individuals and organizations involved in money laundering activities.*[2]*

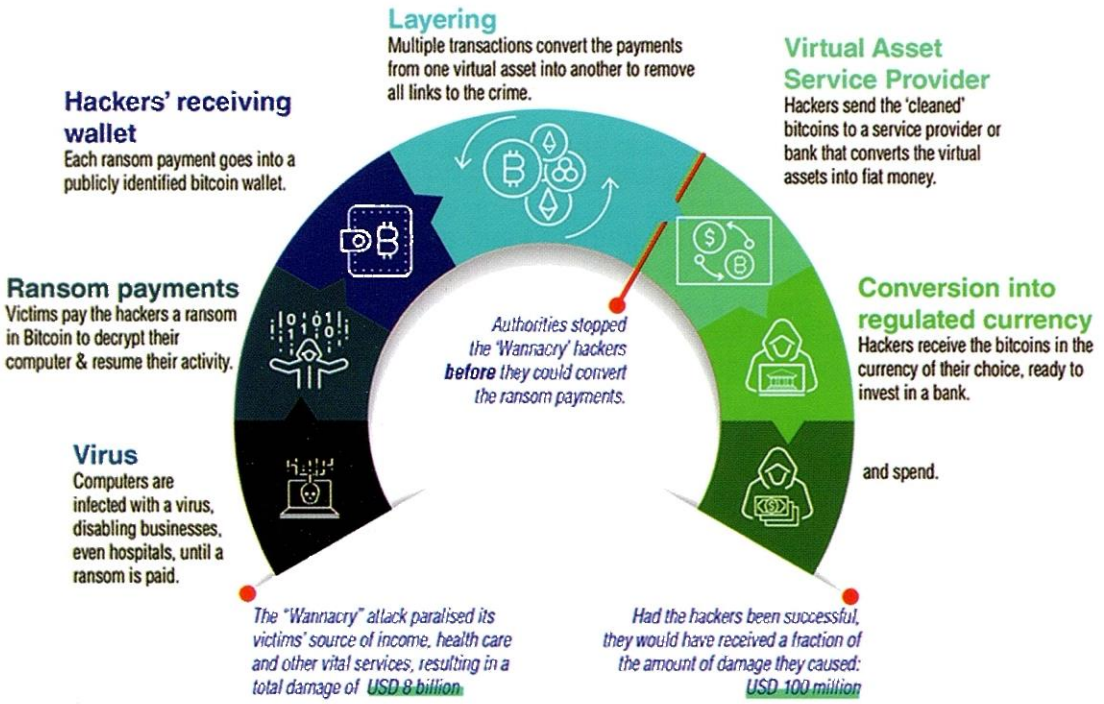


Image Source: https://www.fatf-gafi.org/en/publications/Virtualassets/Virtual-assets.html[3]

Individuals involved in bribery and corruption will constantly seek to exploit new areas and opportunities to offend and launder their corruption proceeds and evade the scrutiny of law enforcement and other government agencies. In present scenario cryptocurrencies like Bitcoin, Ethereum, Dogecoin, Litecoin, Teather, Monero, Dash and Cardano have indeed proven resilient. Investor interest, both retail and institutional, in digital currencies has risen dramatically in recent months as Bitcoin indeed has risen back to all-time high as on December 2021, reaching over $49, $188 and Ethereum to nearly $4000.

In conclusion, investigating cryptocurrency-related crimes is essential to combat the growing use of cryptocurrencies by criminals. It is crucial for law enforcement agencies to develop expertise in this area and collaborate with other international agencies to investigate and prevent cryptocurrency-related crimes.

Before going into the details of crypto-forensics, we should first understand how this crypto currency artifacts will help the investigator.

How a cryptocurrency transaction is performed:

1) A user installs a wallet onto his computer or mobile device and, either through a third-party exchange or a donation from another user.

2) To send some of these coins to another user, he goes into his wallet application and submits a request to transfer a sum of coins to the next user.

3) The payment information is gathered into a block and the block is broadcast to the entire network for verification.

4) If the verification is successful, the new block is added into the block chain, which is a public ledger of all past transactions in the network.

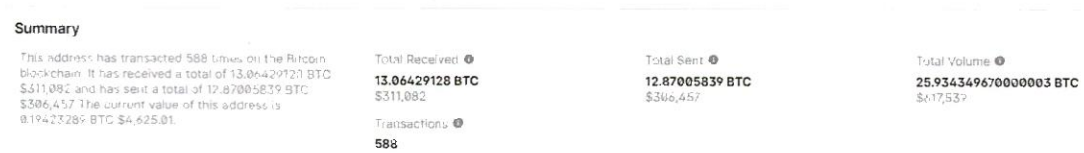
5) Finally, the transferred coins are delivered to the new owner's wallet and the transaction is complete.

Cryptocurrency transactions happen through something called a "cryptocurrency address" or "wallet." These are like account numbers in a bank and keep track of the money and all the transactions done before. If investigators find and look into these addresses early on, it helps them figure out how the money is moving in a case.

In order to make these information/evidence admissible in the court of law, it is very essential to create an exact image of the information and to analyse the information. For this a variety of softwares are used like FTK Imager, Autopsy, etc. Further UFED and Cellebrite software are used for imaging and analysis of mobile devices.

Even though these tools can image the computer/mobile device efficiently, they are unable to identify the cryptocurrency artifacts present in the imaged data. Presently there are no proper tools that that can properly identify the patterns of wallet addresses and transaction hashes.

The typical example of BTC crypto wallet address looks as


Summary

This address has transacted 588 times on the Bitcoin blockchain. It has received a total of 13.06429128 BTC $311,082 and has sent a total of 12.87005839 BTC $306,457. The current value of this address is 0.19423289 BTC $4,625.81.

Total Received
13.06429128 BTC
$311,082

Total Sent
12.87005839 BTC
$306,457

Total Volume
25.934349670000003 BTC
$617,539

Transactions
588

Identifying these early in the case will help the investigator to understand the flow of funds involved in the matter. Artifacts such as wallet.dat files or wallet software such as meta mask or myetherwallet.com could be helpful to recover funds and/or piece together crypto transactions. *[4] [5]*

Cryptocurrency addresses have unique formats that are used as search terms, and even regular expressions can be used for this purpose.

Crypto Address | Bitcoin Address

The Bitcoin address is an identifier of 26-35 alphanumeric characters, beginning with the number 1, 3 or bc1. There are currently three address formats in use:

To prevent confusion, the letters "0," "O," "I," and "l" have been taken out because they can look similar. First, we check if the length of the Bitcoin address is correct.

1. **P2PKH which begin with the number 1**

   1CUfLxoBi5KKaZPDm5rGmqEqTBS28kQkTg

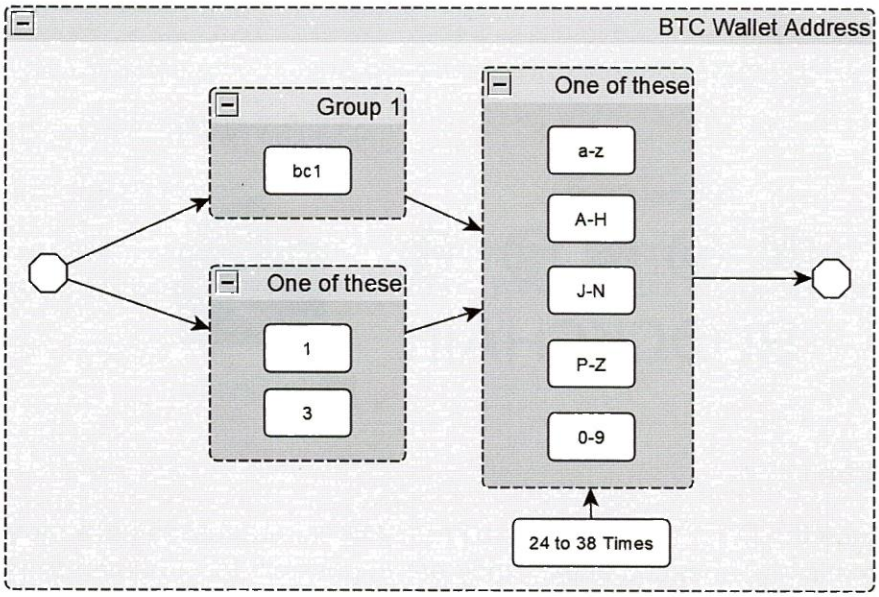
2. **P2SH type starting with the number 3**

   3JmGcSiWRroGHZmZ4uhvM3Rr1ytf4v3uka

3. **Bech32 type starting with bc1**

   bc1q7prqa7r2kjflu02eanudckge0um2v60fncqr4w

Then, we look at the address to see if it has numbers, small letters, or capital letters. After that, we check the starting part of the address. It's important to make sure that only the text with the Bitcoin address is considered.*[6]*



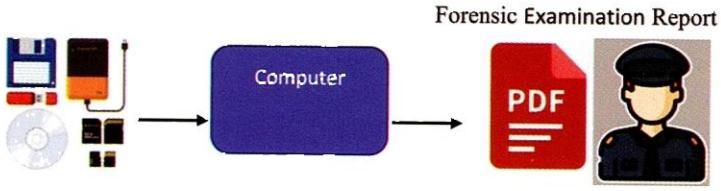
Regular Expression

A regular expression, or regex, is like a special code that helps find specific patterns in text. It's handy for searching or replacing words in a bunch of text, and it's also useful for checking if input (like a password) follows a certain pattern. In an investigation, using regex early on can help find important information, and it stays super helpful as the investigation goes on. *[7]*

Towards Workable Solution

Intelligent use of artificial intelligence and machine learning algorithms was made to produce a powerful solution for the detection of cryptocurrency artifacts and their extraction, enabling the user to precisely identify crypto wallet addresses. It is important to emphasise that the method used in this study is not original; rather, it is a blend of several techniques that have allowed us to achieve our objective.

It is inevitable that it will be included into the field of digital forensics for effective analysis of data due to advancements in artificial intelligence and machine learning algorithms that can read and analyse data on your behalf in a manner similar to a human.



Conclusion

Since the BTC or other cryptocurrency wallet addresses have more than 25 to 45 numeric-alphabet characters, they are impossible for a human to remember.

These wallet addresses can also be stored on any digital device and shared through a variety of channels, including chat, email, messages, and other digital channels. As with many investigations, email and chat-messaging repositories (such as web-based email, Slack, or other chat-messaging platforms like WeChat, WhatsApp, Telegram, Signal, etc.) often help uncover additional parties who may be involved and/or methods for aiding in transaction tracing, in addition to providing additional context and framing around analysis findings. The tool utilises cutting-edge artificial intelligence and machine learning algorithms to read the forensic output file and extract the necessary crypto currency artifacts, placing them into a separate csv file. Such a tool's coding necessitated a heavy reliance on Python and data science algorithms. Within 20 minutes of the tool's operation, the outcome of such crypto wallet data was successfully retrieved from a forensic output file. The process of checking each page for the same data manually might have taken a few months.

The collection and analysis of crypto currency data will be extremely helpful in determining the amount of crypto currency that the accused or suspect is using, as well as in locating the money trail for any crypto-related transactions that the case investigators are currently unaware of.

References:

1. https://www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-assets-red-flag-indicators.html
2. https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf
3. https://www.fatf-gafi.org/en/publications/Virtualassets/Virtual-assets.html
4. https://www.myetherwallet.com/
5. https://metamask.io/
6. Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system (White Paper)." Retrieved from (02-03- 2017): https://bitcoin. org/bitcoin. pdf (2008).
7. Ibid.