A review of research in forensic investigation of cryptocurrencies

Borase Bhushan Gulabrao*

School of Doctoral Studies and Research,
National Forensic Sciences University,
Gandhinagar, Gujarat, India
Email: bhushan.phdcf21@nfsu.ac.in
*Corresponding author

Digvijaysinh Rathod

School of Cyber Security and Digital Forensics,
National Forensic Sciences University,
Gandhinagar, Gujarat, India
Email: digvijay.rathod@nfsu.ac.in

Abstract: In last one decade, use of cryptocurrencies in various fields has increased phenomenally. It offers many benefits to the users. It also has emerged as one of the major challenges for law enforcement agencies across the world. Research has been conducted to identify forensic artefacts for various cryptocurrencies used in different wallets and on different platforms. This paper aims to analyse and sum up the existing literature on forensic investigation of cryptocurrencies. This review paper makes mention of forensic investigation of six different cryptocurrencies, 30 different types of wallets and of 49 different types of forensic artefacts. It also mentions 25 different tools used in forensic investigation. Paper briefs about seven different cryptocurrency *visualisation* and analysis tools. Finally, the paper highlights about research gaps in this field.

Keywords: blockchain; cryptocurrency forensics; forensic artefacts; wallets; Bitcoin; Monero; Verge; Litecoin; Dogecoin; memory forensics; disk forensics; mobile forensics.

Reference to this paper should be made as follows: Gulabrao, B.B. and Rathod, D. (xxxx) ‘A review of research in forensic investigation of cryptocurrencies’, *Int. J. Electronic Security and Digital Forensics*, Vol. X, No. Y, pp.xxx–xxx.

Biographical notes: Borase Bhushan Gulabrao is a PhD student in the School of Doctoral Studies and Research at National Forensic Sciences University, Gandhinagar, Gujarat, India. His areas of interests include study of different types of cryptocurrencies, understanding their transactions and finding out digital artefacts associated with these transactions.

Digvijaysinh Rathod is an Associate Dean and Associate Professor in the School of Cyber Security and Digital Forensics at National Forensic Sciences University, Gujarat, India. He has 19 years of teaching, consultancy and research experience in the domain of cyber security and digital forensics. His areas of interest are ICS/SCSDA security and forensics, web security, mobile security and digital forensics.

1 Introduction

On 3rd January 2009, first Bitcoin was mined and since then as on 31st August 2022, more than 20,000 Cryptocurrencies have come into existence. The market capitalisation of all the cryptocurrencies combinedly has crossed the mark of 1 trillion USD. Nakamoto (2008) defined an electronic coin as a chain of digital signatures. At its core, Bitcoin incorporates the following concepts as mentioned by Champagne (2014).

a A public ledger (called Bitcoin's blockchain). Consider this as an essentially a giant book that is publicly available and contains the bookkeeping records of all transactions ever made in the Bitcoin system, with new pages constantly being added.

b A cryptographic algorithm called asymmetric encryption used for authorisation of transactions.

c A distributed network of nodes that verify and validate Bitcoin transactions and update the public ledger.

Blockchain technology is the basis on which all the cryptocurrencies are operating. Blockchain technology has potential to revolutionise government functioning, business operations and financial transactions. There are challenges too associated with this technology. One of the products of this technology, cryptocurrency, has emerged as a big challenge for law enforcement agencies (LEA) across the world. As per Internet Crime Complaint Centre (ic3) (2022) of FBI, it received complaints reporting loss of worth 1.6 billion USD in 2021 in cases involving cryptocurrencies. Earlier cryptocurrencies were used by hackers for ransomware payments and by criminals operating on dark web. Now cryptocurrencies have become popular among criminals involved in various scams, frauds and schemes. Money laundering is a crime that has international dimensions and ramifications. Analysis of illicit addresses reveal that cybercriminals have successfully laundered 8.6 billion USD worth of cryptocurrency in 2021 as mentioned in the Chainalysis 2022 Crypto Crime Report (n.d.). Worst of all, cryptocurrencies can be used by terrorist organisations. Potential for cryptocurrencies to facilitate terror finance operations are:

a fundraising

b illegal drugs and trafficking of arms

c remittance

d funding of an attack

e funding for operational works as explained by Dion-Schwarz et al. (2019).

In addition to above mentioned crimes, there is a risk of arbitrary content getting uploaded on blockchain. It may lead to violations of copyright, circulation of malware, violations of privacy, uploading of content that can be politically sensitive, etc. Presence of illicit content like child pornography in Blockchain, may make mere possession of blockchain as an offence as explained by Matzutt et al. (2018).

Considering all above-mentioned factors, a lot of research work is desired in understanding the cryptocurrencies. More understanding is desired in finding their patterns in illegal transactions and tracing them to the criminals. The endeavour in this review paper is to present the research work done so far in the field of cryptocurrency forensics so that it is useful to LEA as well as to digital forensic investigators.

Section 2 of the paper mentions about digital forensic studies conducted on various types of cryptocurrencies and the digital artefacts found. Section 3 includes visualisation and investigation tools available for cryptocurrencies. Section 4 highlights about research gaps in the field of cryptocurrency forensics and Sections 5 concludes the paper.

2 Studies on various cryptocurrencies

Research has been conducted on many cryptocurrencies to study the forensic artefacts they leave in RAM, disk and network. The concise observations of the same are mentioned in Table 1.

3 Visualisation and investigation tools for cryptocurrencies

Many visualisation and investigation tools for cryptocurrencies are available either as open-source tool or as a proprietary tool. Some of the tools with their features are explained below.

3.1 BlockQuery

Thomas et al. (2022) describe BlockQuery as an open source blockchain query system for cryptocurrency Bitcoin. Many tools are not capable of detecting transactions generated by Hierarchical Deterministic wallets due to failures in their address derivation methods. The authors claim that the BlockQuery is capable of detecting same. The authors mention that for examination of cryptocurrency to be forensically sound, it must meet criteria like completeness, integrity and confidentiality. LEA need to be careful as any compromised query service may associate their IP address with wallet query to identify wallets under scanner. Extended keys can be very helpful in associating different transactions to a single point of origin. Hierarchical Deterministic wallets use extended keys to categorise addresses under logical accounts. There are three valid Bitcoin address representations – P2PKH, P2SH, P2WPKH. Each Bitcoin address type has a corresponding extended key representation used to derive addresses of that type. All three Bitcoin address types are used by some hierarchical deterministic wallet implementations such as Ledger Live. The software architecture of BlockQuery comprises of a Bitcoin node, Indexer and Web Application as shown in Figure 1. The paper mentions the comparison of BlockQuery tool with other open-source Hierarchical Deterministic wallet lookup tools like Blockchair.com, Blockchain.info, Blockchainexplorer.one, Blockpath, LedgerHQ, xpub-scan, dan-da, hd-wallet-addrs, mewald55, Blocknomics.co. It evaluated their performance on parameters like adjustable depth, automatic conversion, open source and confidentiality.

Table 1 Artefacts of different cryptocurrencies

	Cryptocurrency, OS and tools	*Wallets used*	*Forensic examination*	*Observations and artefacts found*	*Reference*
1	Monero (Ubuntu Operating system)	Monero GUI v0.11.1.0	Memory	Public address of a transaction, transaction id, Passphrase, public address of wallet, mnemonic seed	Koerhuis et al. (2020)
			Disk	Transaction id, public address of wallet, transaction amounts, public address of a transaction	
			Network	Indicators of use	
2	Verge (Ubuntu Operating system)	Verge v4.0.2.0	Memory	Labels, transaction amount, stealth address, Passphrase, public address of wallet, public address of a transaction,	Koerhuis et al. (2020)
			Disk	Stealth address, transaction id, transaction amounts, public address of wallet, public address involved in transaction	
			Network	Nil	
3	Litecoin	Litecoin wallet v.3.3.0.9	*Four stages*	*Physical android device results*	Montanez (2014)
	Darkcoin	Darkcoin wallet	1 Before wallet installation	1 Installed applications.	
	Bitcoin	Beta v.1.0.1	2 After installation	2 Identifier	
	OS – (Android OSv.4.4.2)	Hive Bitcoin wallet v.0.3.3.3.46	3 After transaction	3 Purchase date and time (installation date)	
	Samsung Galaxy S4	Bitcoin wallet V3.53	Completion	4 launcher.db file – app order and favourites tables	
	Model GT-19500		4 After deleting the application	5 localappstate.db file – identifiers, first download timestamps, most recent data delivery timestamp, user account in which it was downloaded	
	Tool – UFED			6 Timeline data table – timestamps	
				7 finsky.xml file in com.android.vending sub-item – it is record of application update notifications	
	Bitcoin	bitWallet (v. 1.5)	*Four stages*	*Physical iOS device – UFED analyser results*	Montanez (2014)
	OS – (iOS – Apple iPhone 4 Model A1332) iOS v.7.1.1)	Coin pocket (v. 1.1.0)	1 Before wallet installation	1 Installed applications – extraction table shows entries for both wallets as well as identifier.	
	Tools – UFED		2 After installation	2 Configurations – .plist, storage path of .plist configuration files, date and time stamps found for CoinPocket wallet	
	iFunBox – open source app/file manager for iOS devices		3 After transaction	3 No configuration files found for bitWallet	
			Completion	4 Database category – two databases with coin pocket identifier – cache database and local storage file. No entries found for bitWallet	

Table 1 Artefacts of different cryptocurrencies (continued)

	Cryptocurrency, OS and tools	*Wallets used*		*Forensic examination*		*Observations and artefacts found*	*Reference*
	iFunBox – open source app/file manager for iOS devices	Coin pocket (v. 1.1.0)	4	After deleting the application		*Physical iOS device – iFunBox analyser results*	Montanez (2014)
					1	Wallet application dump of bitWallet – five folder are found – bitWallet.app, documents, library, StoreKit and tmp	
					2	Documents folder has alerts.file. It has public address string of wallet	
					3	Same folder has file named as wallets.v1. This file listed public address key as well as private key	
					4	Wallet application dump of coin pocket has same five folders but none of these files and folders has relevant forensic data.	
4	Dogecoin and Bitcoin	Coinbase v1.22.3	1	Transactions done from cold wallet to installed wallets		*Observations*	Chang et al. (2022
	OS – Android OS	Coinomi v9.26.3			1	Coinomi wallet application stored the hash ID as human readable text in Android file system.	
	Samsung Galaxy Phone S 9 + SM-G965U Android 8.0 Oreo *Tools* – Cellebrite UFED touch 2.0, Cellebrite Physical analyser, Cyphertrace	Atomic v.0.75.1	2	Artefacts searched – Hash ID, addresses, cookies and Oauth password artefacts	2	Coinomi wallet application provided the hash ID for Bitcoin and Dogecoin wallets and were found in the path of the cache folder. The wallet application creates a folder titled by a unique hexadecimal string in the path: /data/com.coinomi.wallet/cache/f78fc8de58b92a6f/bitcoin.main/<HASH ID>. Same applies to dogecoin too.	
					3	Coinbase wallet requires e-mail address to create an account considering the application is not a proprietary wallet application and also provides exchange services. For every transaction, user receives an e-mail from the exchange from id no-reply@coinbase.com.	
					4	No cookies were found for Coinomi wallet application.	
					5	Atomic wallet application revealed 16 cookies captured. The web cookie file path for the Atomic wallet application was found in: *userdata(ExtX)/Root/data/io.atomicwallet/app_webview/Default/Cookies*	
					6	The Cloudflare cookie was created after the installation of atomic wallet.	
					7	Six cookies were identified which revealed that Coinbase also used services of Cloudflare	
					8	OAUTH artefacts – 208 password files were acquired in the extraction of the test device with physical extraction. 185 are based on OAuth 2.0 protocol managed by google and there was no implementation of OAuth tokens by installed wallet applications.	

Table 1 Artefacts of different cryptocurrencies (continued)

	Cryptocurrency, OS and tools		*Wallets used*		*Forensic examination*			*Observations and artefacts found*	*Reference*
4	*Tools* – Cellebrite UFED touch 2.0, Cellebrite Physical analyser, Cyphertrace			2	Artefacts searched – Hash ID, addresses, cookies and Oauth password artefacts	9		Cellebrite cloud analyser (CA) forensically captures data from the cloud-based applications installed on mobile devices. CA captured 4 bitcoin transactions but did not capture any dogecoin transaction.	Chang et al. (2022
						10		Cellebrite supports only Coinbase and not Coinomi or Atomic wallet applications.	
						11		Bitcoin.main and Dogecoin.main folders were created that contained 0 kb files labelled with hash IDs.	
						12		Dogecoin has been a popular coin in mainstream media and not a lot is known about this cryptocurrency in academic research due to sheer volume of coin types.	
						13		HTTP cookies and OAuth tokens were examined but provided no relevant data towards attribution.	
5	Bitcoin		*Wallets used*		*Browsers*			*Observations*	Zollner et al. (2019)
	OS – Windows 7 and Windows 10		*Client wallets*	1	Tor	1		For client type wallets paper mentions about	
	Tools	1	Armory	2	MS Edge		a	Common artefacts– client type, default directory, process name	
	1 WinBAS – Windows Bitcoin Artefacts Scanner	2	Multibit HD	3	Mozilla Firefox		b	Specific artefacts – 32-bit specifics and 64-bit specifics	
	2 fssearch.py	3	Electrum	4	Internet Explorer		c	After uninstalling artefacts – files, cookies, history, login data etc.	
	3 For RAM – Winpmem_1.6.0.exe16	4	mSIGNA	5	Google Chrome	2		For web wallets, browser artefacts found are mentioned below	
	RawCopy.exe	5	Bitpay		*Modes* – normal and incognito		a	Normal mode – history, cookies, cache, bookmarks, favourites, login data like wallet ID, e-mail, mnemonic and passwords	
	RawCopy64.exe	6	Bither		Using the tools mentioned, various artefacts are collected and analysed		b	Incognito mode – RAM provides URLs, passwords, mnemonics and wallet IDs.	
	4 WebBrowserPassView tool from Nirsoft	7	Bitcoin Core			3		Automated tool used found eight different addresses and keys	
	5 WinPrefetchView	8	Bitcoin knots			4		Use of browser or client can be identified by use of prefetch files	
	6 List of Bitcoin keywords (34)		*Web wallets*			5		Evidence of uninstallation is also useful in investigation	
	7 List of Bitcoin file signatures	1	Blockchain			6		RAM, pagefile.sys and hiberfil.sys are rich source of evidence	
		2	bitgo			7		Mnemonic code words may sometimes found in the RAM after the password	

Table 1 Artefacts of different cryptocurrencies (continued)

	Cryptocurrency, OS and tools	*Wallets used*	*Forensic examination*	*Observations and artefacts found*	*Reference*
5	7 List of Bitcoin file signatures	3 coin.space 4 greenaddress 5 coinapult 6 coinbase 7 xapo		7 Mnemonic code words may sometimes found in the RAM after the password	Zollner et al. (2019)
6	Bitcoin	*Wallets used*	*Browsers*	*Observations*	Thomas et al. (2020)
	OS – Windows 7	1 Ledger Nano X 1.2.4-1	1 Mozilla Firefox 71.0	1 Relevant data structures are identified using cheat engine.	
	64 bit	2 Trezor One 1.8.3	2 Google Chrome 79.0.3945.88	2 API requests also analysed	
	Tool	Application		*Artefacts found*	
	1 FORESHADOW – Plugin software that can be used for memory analysis	Ledger Live v.1.18.2		a LedgerLive – wallet addresses, device metadata, public keys, transaction history	
	2 YARA Scans	Trezor wallet1.8.3		b Trezor wallet – public keys, device metadata, extractable password, Transaction history and wallet addresses.	
	3 Open source visualisation framework and algorithm	Trezor Bridge 2.0.27		c All extended public keys synced with the client could be located using regular expression based YARA scans.	
		Volatility 2.6		d The persistence of memory artefacts is extremely poor in Ledger.	
		Cheat Engine 7.0		e Certain artefacts in memory which persisted for long even after its browser tab was killed could be seen in Trezor wallet client	
				f Even after the termination of the process, extended public keys remained in memory without being corrupted. The derivation of all past and future wallet addresses can be done from extended public key.	
				g Once the application is terminated, the Passphrase artefacts were overwritten immediately.	
7	Bitcoin	*Client-based wallets*	*Memory forensic examination*	*Observations*	Van Der Horst et al. (2017)
	OS – Microsoft Windows 7 Enterprise	1 Bitcoin Core v0.11.1	Memory images are taken as below	Bitcoin Core – Berkeley database is used to store keys and user data. Berkeley database is written in C and stores key material in the form of binary data. Bitcoin core allows the user to make a backup of a wallet file to a location on disk.	

Table 1 Artefacts of different cryptocurrencies (continued)

Cryptocurrency, OS and tools	*Wallets used*	*Forensic examination*	*Observations and artefacts found*	*Reference*
7 *Tools*	2 Electrum v2.6.2	Bitcoin Core	Electrum – JSON format is used to store data in a file and text-based data is used to store key material.	Van Der Horst et al. (2017)
1 VM Ware fusion professional edition v		1 Unused client	*Artefacts*	
2 Memory images are analysed using Volatility v2.5 and standard Linux command line tools in a virtual machine running Kali GNU/Linux v2.0		2 Used client unencrypted	Bitcoin Core	
		3 Used client encrypted	1 When wallet used is unencrypted, all known private keys are located in binary format to process memory. Private keys could not be traced back in memory.	
		4 Used client after reboot	2 Private keys in wallet import format could not be located.	
3 Yarascan plugin		Electrum	3 Process memory in all images had all known public keys in binary format.	
4 Netscan plugin		1 Unused client	4 All memory images had known labels.	
		2 Used client encrypted	5 Memory image also had transaction ID	
		3 Used client after reboot	6 Process memory did not have passphrase used for wallet encryption	
			7 User specified file location had a backup wallet file.	
			8 Format – public keys and private keys are found in binary format. Labels, Addresses, transaction IDs, file locations appear as string values in memory.	
			9 Private keys are preceded by the fingerprint 0xf70001d63081d30201010420	
			10 Two different fixed strings key! And keymeta! preceded all known public keys in binary format. Fingerprints name' and purpose' also preceded in one instance. Analysis shows that these are the Berkeley database tags for the wallet.dat file and public keys.	
			11 One transaction ID was preceded by the string 'AddToWallet' This string can be found in debug.log when new transaction ID is added to the wallet.	
			12 wallet.dat file is the keystore containing the bitcoin keys and all user data. The debug.log file shows the transactions initiated by wallet with their date and time. It also shows the file location of any backup created by user.	

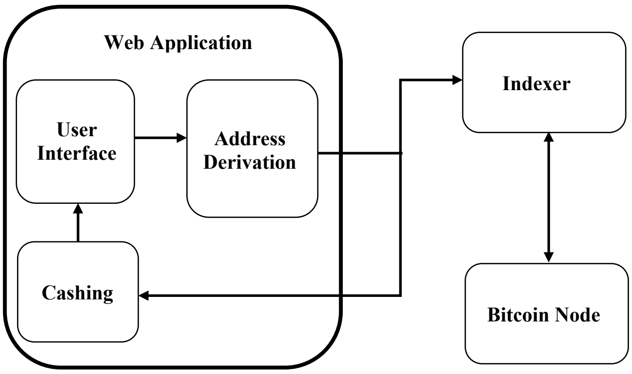
Table 1 Artefacts of different cryptocurrencies (continued)

Cryptocurrency, OS and tools			*Wallets used*		*Forensic examination*		*Observations and artefacts found*		*Reference*
7	4	Netscan plugin	2	Electrum v2.6.2	3	Used client after reboot	13	Handles plugin is used to identify registry keys used by the Bitcoin Core client. Presence of an active instance of Bitcoin Core client can be identified by the presence of these keys.	Van Der Horst et al. (2017)
							14	An overview of the connection objects encountered in memory image can be seen from netscan plugin.	
							Electrum		
							1	Process memory did not have any private key or checksum of private key.	
							2	Process memory has all known values of the public key as well as the master public key.	
							3	Process memory has all known labels	
							4	All know transaction ID were found in process memory	
							5	Process memory did not have Passphrase of the wallet	
							6	One of the memory images had full path of the backup file location	
							7	Format – most of the data appeared as string values in memory. But Public keys associated key pairs involved in wallet transactions occurred in binary format.	
							8	The involvement of the key in transaction can be seen from the presence of binary public keys in process memory.	
							9	The user and the key data can be seen ordered with various tags in JSON file located in wallet file.	
							10	The string blockchain.address.subscribe preceded all public key addresses associated with key pairs in the wallet. This string is associated with protocol between Electrum server and Electrum client.	
							11	The key material, user data and transaction history can be located in electrum wallet file. Wallet backups can only be attributed to the electrum process by manually analysing the file paths in process memory.	
							12	Application specific registry key was not found in use.	
							13	TCP port 50003 and TCP port 443 are visible in memory image with netscan plugin. Their presence indicates presence of electrum application.	

Table 1 Artefacts of different cryptocurrencies (continued)

	Cryptocurrency, OS and tools	*Wallets used*	*Forensic examination*	*Observations and artefacts found*	*Reference*
8	Bitcoin	*Mobile wallets*	Artefacts analysis has been done manually on the files extracted. Artefacts like wallet private keys, seed, transaction history, application specific data including password, Pin were searched	*Observations*	Haigh et al. (2018)
	OS – Android version 4.4 (Kitkat) on Samsung Galaxy S3 and Linux on Laptop to retrieve and analyse data.	1 Coinbase		1 Coinbase – this wallet keeps private keys and most wallet data on server. The shared_prefs XML file has plaintext password. It also contains preferences and various options for the application. Transaction and accounts databases have data items such as account balances, transaction amounts and account ids.	
	Tools	2 Binance		2 Binance – no sensitive information is stored on device but on their servers. No transaction history is stored in the device.	
	1 Bitcoinj wallet tool	3 Bitcoin wallet		3 Bitcoin wallet – the private keys and seed associated with the wallet and complete transaction history can be found by using Bitcoinj wallet tool.	
	2 Monkeyrunner	4 Xapo		4 Mycelium – SQLite database is used to stores its transaction data in encrypted form.	
	3 Text editor	5 Mycellium		5 XAPO – private keys are stored on cloud and not on physical device. It also stores a plaintext database that comprises of transactions history.	
	4 SQLite database browser	6 Bitpay		6 Bitpay – File com.bitpay.wallet/files/profile had wallet keys. com.bitpay.wallet/files/txsHistory-<wallet-id> had transaction history.	
	5 Android Debug Bridge	7 Coinpaymen ts		7 Coinpayments – net.coinpayments.coinpaymentsapp /app webview/databases/file 0 had a database that comprised of API public/private key pair.	
9	Bitcoin	*Desktop wallets*	1 Signature snapshots are taken at various stages	*Observations*	Ngwu et al. (2021)
	OS – Windows 10	1 Multibit HD		Searches are made in	
	Tools	2 Electrum		1 RAM	
	1 VM	3 Armory		2 Program files	
	2 OS Forensics	4 mSIGNA	2 System is restarted after wallet installation, after the transaction, after deletion of the app and data is captured to check the artefacts	3 Hard disk	
	3 Magnet RAM capture	5 Bitpay		4 App data folder	
	4 hex editor HxD	6 Bither		5 Backup file	
				6 Log file	
				7 Executable file	
				8 Registry	
				Artefacts like private key, public key, seed phrase, password, PIN, transaction ID, transaction history, PII are searched	

Figure 1 Software architecture of BlockQuery



3.2 Blockchain explorer

Kuzuno and Karam (2017) propose a practical Bitcoin analytical process and combination of methods to search specific known address activities analyse the transaction history. It is also proposed to identify relation between two addresses and cluster sets of known addresses. They propose Blockchain Explorer as three-part system.

1 Indexer – it builds an Index of addresses and transactions.

2 Linking of tag from suspicious addresses reported to system from law enforcement.

3 A function providing statistics and information in relation to given address.

4 Visualiser to show address relationship of transactions.

5 It uses finder that will discover the transaction path in any address. It also does clustering of multiple addresses that may belong to one wallet.

6 Web interface for the user.

This paper discusses about analysis of three real life cases of Silk Road, Cryptolocker ransomware and DD4BC extortion case.

3.3 Visualising dynamic Bitcoin transaction pattern

McGinn et al. (2016) describe a systematic top-down visualisation of Bitcoin transaction activity to explore dynamically generated patterns of algorithmic behaviour. Such patterns are of importance for financial regulators, protocol designers and security analysts. These visualisations have revealed the structure of recurring high frequency pattern of an algorithmic denial of service attack on Bitcoin system. It has also provided recurring pattern of money laundering.

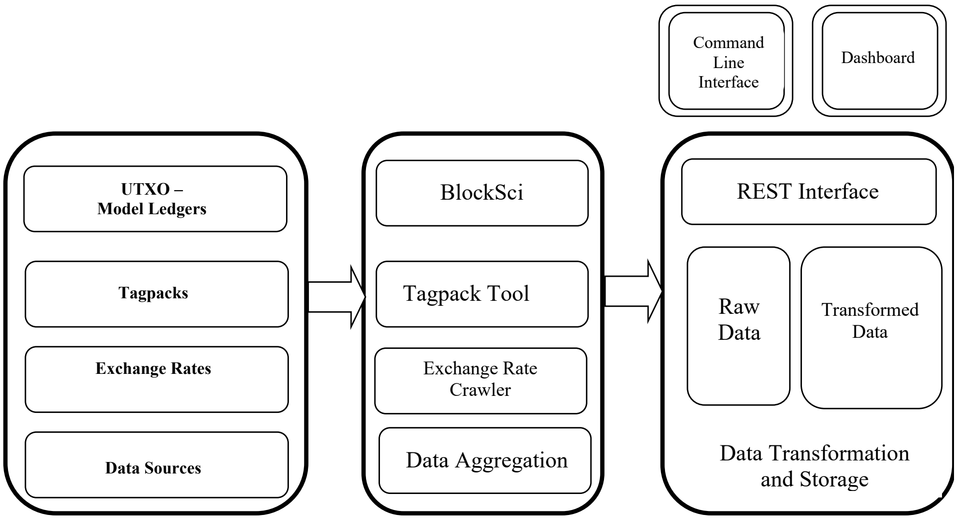
3.4 Quantitative analysis

Ron and Shamir (2018) explain about analysis of behaviour of Bitcoin users like how they acquire, how they spend and how they transfer Bitcoins between their various accounts for protection of their privacy. In order to find sets of addresses which are expected to belong to the same user, the authors have used union-find graph algorithm. The original transaction graph is called as address graph and the contracted transaction graph is called as the entity graph. The paper shares the statistics related with number of addresses, accumulated incoming Bitcoins and number of transactions for exchange Mt. Gox, Instawallet and Deepbit wallet.

3.5 GraphSense

Haslhofer et al. (2021) mention that GraphSense platform can be used for executing advanced analytics tasks using a standard data science tool stack. It can also be used for interactive investigations of monetary flows. It is an open-source software. It provides analysis for *Bitcoin, Bitcoin Cash, Litecoin and Zcash*. The architecture of the GraphSense is given below

Figure 2 GraphSense architecture



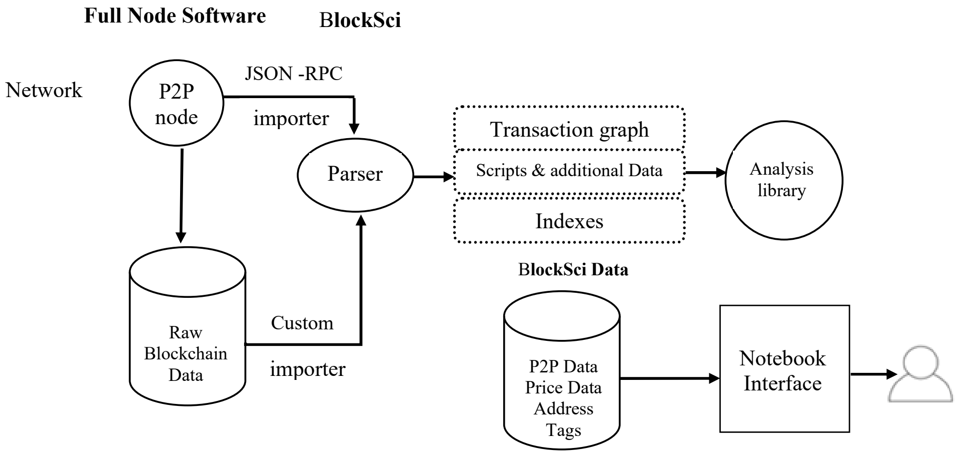
It implements the co-spent heuristics which is also known as multiple input heuristics. It does not use change heuristics. As per this paper as on 19.02.2021, there are 671,193 Blocks, 617,563,419 transactions, 786,122,678 addresses and 5,858 tags. This project maintains an elaborate mechanism to collect attribution tags and name them as TagPacks.

3.6 BlockSci

Kalodner et al. (2020) describe BlockSci as an open-source platform for analysis of Blockchain. It supports blockchains of Bitcoin, Bitcoin Cash, Bitcoin SV, Litecoin and Zcash. The architecture is given below.

It has library of tools that can identify coinjoin transactions and linking of addresses by known heuristics. Some analyses given are – 88% of inputs spend outputs created in last 4,000 blocks, i.e., in 27.77 days average. Only 8.6% Bitcoin addresses are used more than once but those account for 51% of all occurrences.

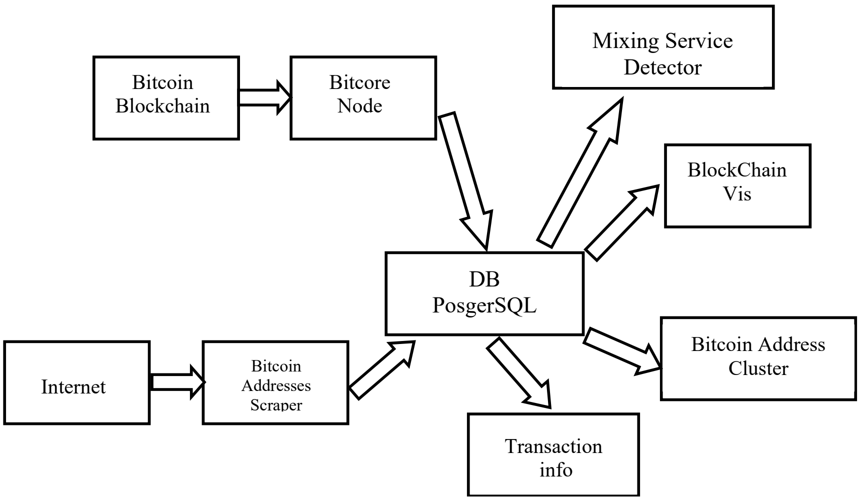
Figure 3 BlockSci architecture



3.7 *BlockChainVis suite of tools*

Bistarelli et al. (2018) propose the tool for forensic analysis of the Bitcoin blockchain. The tool architecture is given in Figure 4.

Figure 4 BlockChainVis suite of tools



This tool comprises three different virtual machines running:

1 Bitcoin core

2 PostgreSQL

3 Software dedicated for visualisation of web applications.

The tool uses Bitcoin address scrappers to build lists of mining pool addresses, online wallet addresses, gambling addresses and addresses that were seized by law enforcement authorities. The Bitcoin addresses clusterer uses following – the multi-input heuristics, the shadow heuristics, the consumer heuristics, the optical change heuristics, one-to-one heuristics, multisig-one heuristics and multisig-two heuristics.

3.8 Cryptocurrency wallets comparison

Suratkar et al. (2020) have studied web wallets, mobile wallets, desktop wallets and hardware wallets on following parameters – supported coins and tokens, key management, fiat currency option, anonymity, platform support and wallet recovery method. According to authors, the best wallets as per above mentioned criteria are mentioned in Table 2.

Table 2 Best wallets for cryptocurrencies

Type of wallet		*Name of wallet*	*Coins and token supported*
1	Web-based wallet	Jaxx	78
		Guarda	49
2	Mobile wallet	Coinomi	120
3	Desktop wallet	Atomic	300
4	Hardware wallet	Ledger Nano S	1,310

4 Research gaps in the field of cryptocurrency forensic research

1 Research gaps in Bitcoin forensics as mentioned by Zollner et al. (2019) are

- the analysis of different formats of keys and addresses
- the combination of live and postmortem forensics
- analysing the file signatures of Bitcoin relevant files
- The analysis of most used Bitcoin clients to find more artefacts on the file systems and registry.

2 BTCscan is a Python script. It automates the extraction of Base58Chek encoded strings that meet the format of the Bitcoin from any file that the script is run over as explained by Cowen (2015). Similar tools are required for other popular cryptocurrencies used by criminals.

3 Query by extended public key is not supported by many existing Bitcoin transaction lookup tools. Such tools also fail sometimes to produce the same wallet addresses as those derived by HD wallets as explained by Haigh et al. (2018).

4 There is a lack of an open source extended key dataset. Such dataset would greatly facilitate the development of more forensic tools leveraging extended keys as explained by Haigh et al. (2018).

5 Numerous international organisations have produced excellent research work on money laundering and terrorism financing methods and techniques. It is available in

the form of annual reports and annual typology reports. These reports, which contain details of sanitised, successfully detected money laundering and terrorism financing cases, provide a wealth of information on current threat and trends, techniques employed, the amount of funds involved. There is no such reference work, red flag indicator or behaviour models that would assist LEA, financial intelligence units, digital wallet providers or exchanges to determine suspicious behaviour linked to the use of cryptocurrencies for malicious purposes as mentioned by Irwin and Turner (2018).

6 There are no efficient approaches for extracting forensic artefacts existing on mobile devices cryptocurrency wallet application. There has been no research focused on web-based cookies and Oauth tokens in the context of cryptocurrency wallet forensic analysis. Single sign on (SSO) is also a topic of research as explained by Chang et al. (2022).

7 How cookies and tokens interact between wallet application and Android is a topic that has not been researched in the context of forensic artefact discovery and attribution as explained by Chang et al. (2022).

8 Conducting network analysis in behaviour of cookies and Oauth tokens in modern wallet applications could provide valuable network data such as IP, addresses, credentials for attribution as explained by Chang et al. (2022).

9 Very little research has been done in Dogecoin as explained by Chang et al. (2022).

10 Cloudflare claims that all the data (not content) flows through their computing technology can provide attribution in cryptocurrency investigation as explained by Chang et al. (2022). This claim needs to be leveraged for attribution.

11 An implementation of an international understanding and a legal framework to regulate cryptocurrency will help in better efficacy in combating cryptocurrency-related crime as described by Tziakouris (2018).

12 Artificial intelligence (AI) techniques particularly explainable AI may be used to facilitate evidence search. There is potential for research in this area as mentioned by Zollner et al. (2019).

13 Van Der Horst et al. (2017) proposed that research may be conducted to forensically examine newer versions of Bitcoin clients with the aim of proposing a forensic taxonomy of Bitcoin client artefacts.

14 Out of roughly 251 million transactions on Bitcoin blockchain, about 1.4% of them carry arbitrary data. If Illegal content or data causing serious privacy violations is uploaded on any blockchain, it may cause serious problems for the entire blockchain ecosystem as mentioned by Roman et al. (2018). A mechanism of monitoring such arbitrary data and stopping uploading of such data can be a big research challenge.

5 Conclusions

The Blockchain technology has opened many opportunities for governments, businesses as well as entrepreneurs. At the same time, its products like cryptocurrencies and tokens are going to make job of LEA more and more difficult. Technical nature, lack of regulations, procedural hassles in international data sharing, lack of central coordinating body, lack of central database of tainted cryptocurrencies are some of the challenges for LEA. The paper has shown the progress made in cryptocurrencies forensic investigations so far and it also shows that much more research is desired in this field to keep LEA one step ahead of criminals. Multiple variables like more than 20,000 cryptocurrencies, more than 500 exchanges, presence of services like mixers, varieties of wallets, operating systems, etc. would require presence of multiple Standard Operating Procedures in identification, preservation, collection and analysis of digital evidence related with cryptocurrencies. More research is desired in digital forensics of cryptocurrencies, tokens, NFT's and CBDC in anticipation that use of these products in crime will increase over the years. The research should bring out the keyword dictionary, taxonomy and good procedures associated with digital examination. This filed is very fast evolving and more and more people are working to increase anonymity associated with these products. Researchers also need to match the pace and evolve new methodologies and techniques to examine crypto assets forensically.

References

Bistarelli, S., Mercanti, I. and Santini, F. (2018) 'A suite of tools for the forensic analysis of bitcoin transactions: preliminary report', *Lecture Notes in Computer Science*, pp.329–341, DOI: 10.1007/978-3-030-10549-5_26.

Chainalysis 2022 Crypto Crime Report (n.d.) [online] https://go.chainalysis.com/2022-crypto-crime-report.html p.11 (accessed 31 August 2022).

Champagne, P. (2014) *The Book of Satoshi: The Collected Writings of Bitcoin Creator Satoshi Nakamoto*, p.10, E53 Publishing LLC.

Chang, E., Darcy, P., Choo, K.K.R. and Le-Khac, N.A. (2022) *Forensic Artefact Discovery and Attribution from Android Cryptocurrency Wallet Applications* https:://doi.org/10.48550/axXiv.2205.14611.

Cowen, C. (2015) *Forensics and Bitcoin, Forensic Focus* [online] http://articles.forensicfocus.com/2015/01/16/forensics-bitcoin/.

Dion-Schwarz, C., Manheim, D. and Johnston, P. (2019) *Terrorist Use of Cryptocurrencies Technical and Organizational Barriers and Future Threats*, pp.34–35, RAND Corporation, Santa Monica, Calif., DOI: https://doi.org/10.7249/RR3026.

Haigh, T., Breitinger, F. and Baggili, I. (2018) *If I had a Million Cryptos: Cryptowallet Application Analysis and a Trojan Proof-Of-Concept*, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp.45–65, DOI: 10.1007/978-3-030-05487-8_3.

Haslhofer, B., Stütz, R., Romiti, M. and King, R. (2021) *GraphSense: A General-Purpose Cryptoasset Analytics Platform* [online] https://arxiv.org/abs/2102.13613 (accessed 31 August 2022).

Internet Crime Complaint Centre (ic3) (2022) | Annual reports. (n.d.) [online] https://pdf.ic3.gov/2012_IC3Report.pdf, pp.13 (accessed 31 August 2022).

Irwin, A.S. and Turner, A.B. (2018) 'Illicit bitcoin transactions: challenges in getting to the who, what, when and where', *Journal of Money Laundering Control*, Vol. 21, No. 3, pp.297–313, DOI: 10.1108/jmlc-07-2017-0031.

Kalodner, H., Möser, M., Lee, K., Goldfeder, S., Plattner, M., Chator, A. and Narayanan, A. (2020) '{BlockSci}: design and applications of a blockchain analysis platform', *29th USENIX Security Symposium, USENIX Security*, Vol. 20, pp.2721–2738.

Koerhuis, W., Kechadi, T. and Le-Khac, N. (2020) 'Forensic analysis of privacy-oriented cryptocurrencies', *Forensic Science International: Digital Investigation*, Vol. 33, p.200891, DOI: 10.1016/j.fsidi.2019.200891

Kuzuno, H. and Karam, C. (2017) 'Blockchain explorer: an analytical process and investigation environment for bitcoin', *APWG Symposium on Electronic Crime Research (eCrime)*, DOI: 10.1109/ecrime.2017.7945049.

Matzutt, R., Hiller, J., Henze, M., Ziegeldorf, J.H., Hohlfeld, O. and Wehrle, K. (2018) 'A quantitative analysis of the impact of arbitrary blockchain content on Bitcoin', in Meiklejohn, S. and Sako, K. (Eds.): *Financial Cryptography and Data Security. FC 2018. Lecture Notes in Computer Science*, Vol. 10957, pp.420–438, Nieuwpoort, Cura, https://doi.org/10.1007/978-3-662-58387-6_23.

McGinn, D., Birch, D., Akroyd, D., Molina-Solana, M., Guo, Y. and Knottenbelt, W.J. (2016) 'Visualizing dynamic Bitcoin transaction patterns', *Big Data*, Vol. 4, No. 2, pp.109–119, DOI: 10.1089/big.2015.0056

Montanez, A. (2014) *Investigation of Cryptocurrency Wallets on IOS and Android Mobile* [online] https://www.marshall.edu/forensics/files/Montanez-Angelica_Final-Research-Paper.pdf (accessed 31 August 2022).

Nakamoto, S. (2008) 'Bitcoin: a peer-to-peer electronic cash system', *Decentralized Business Review*, October, Vol. 21260, p.2.

Ngwu, C.R., Amah N.L. and Ede, C.C. (2021) 'Digital forensic investigation and analysis of bitcoin wallets: data remnants and traces on user machines', *Umudike Journal of Engineering and Technology*, June, Vol. 7, No. 1, pp.79–89, Michael Okpara University of Agricuture, Umudike, https://doi.org/10.33922/j.ujet_v7i1_12.

Ron, D. and Shamir, A. (2013) 'Quantitative analysis of the full bitcoin transaction graph', *Financial Cryptography and Data Security*, pp.6–24, DOI: 10.1007/978-3-642-39884-1_2.

Suratkar, S., Shirole, M. and Bhirud, S.G. (2020) 'Cryptocurrency wallet: a review', *4th International Conference on Computer, Communication and Signal Processing (ICCCSP)*, pp.1–7.

Thomas, T., Edwards, T. and Baggili, I. (2022) 'BlockQuery: toward forensically sound cryptocurrency investigation', *Forensic Science International: Digital Investigation*, Vol. 40, p.301340, DOI: 10.1016/j.fsidi.2022.301340.

Thomas, T., Piscitelli, M., Shavrov, I. and Baggili, I. (2020) 'Memory foreshadow: memory forensics of hardware cryptocurrency wallets – a tool and visualization framework', *Forensic Science International: Digital Investigation*, Vol. 33, Supplement, p.301002, DOI: 10.1016/j.fsidi.2020.301002

Tziakouris, G. (2018) 'Cryptocurrencies – a forensic challenge or opportunity for law enforcement? an Interpol perspective', *IEEE Security & Privacy*, Vol. Vol. 16, No. 4, pp.92–94, DOI: 10.1109/msp.2018.3111243

Van Der Horst, L., Choo, K.R. and Le-Khac, N. (2017) 'Process memory investigation of the bitcoin clients electrum and Bitcoin core', *IEEE Access*, Vol. 5, pp.22385–22398, DOI: 10.1109/access.2017.2759766.

Zollner, S., Choo, K-K.R. and Le-Khac, N-A. (2019) 'An automated live forensic and postmortem analysis tool for bitcoin on windows systems', in *IEEE Access*, Vol. 7, pp.158250–158263, DOI: 10.1109/ACCESS.2019.2948774.