Forensics investigation comparison of privacy-oriented cryptocurrencies

Marija Taneska, Jovana Dobreva, Vesna Dimitrova
Faculty of Computer Science and Engineering, University Ss. Cyril and Methodius
Skopje, Republic of North Macedonia
jovana.dobreva@finki.ukim.mk

Abstract: *Digital cryptocurrencies especially privacy-oriented cryptocurrencies over the past years have experienced significant growth in terms of usage. The increased usage of privacy-oriented cryptocurrencies due to the offered privacy and anonymity, allows a cybercriminal to commit illegal transactions that are harder to trace back than Bitcoin. In this paper, we provide a forensic overview of the privacy-oriented cryptocurrencies Monero, Verge, Dash, and Zcash. We analyse forensics experiments with these cryptocurrencies and make some assumptions and conclusions related to the analysed experiments.*
Keywords*: cryptocurrencies, privacy-oriented cryptocurrencies, forensic, Monero, Verge, Dash, Zcash.*

1. Introduction

Forensic is the science of collecting and examining data to extract useful information related to the cases under investigation. Digital forensic science is a branch of forensic science that focuses on the uncovering, investigation, and interpreting of digital (electronic) data related to (cyber)crime. The forensics investigator is the person initially responsible for examing the evidence. Blockchain forensics and cryptocurrency forensics accounting involve both tracking and interpreting the flow of cryptocurrency assets on blockchains.

Cryptocurrencies have no generally accepted definition in the regulatory space. Prof. Dr. Robby Houben and Alexander Snyer define cryptocurrency as a "digital representation of value that is intended to constitute a peer-to-peer ("P2P") alternative to government-issued legal tender, is used as a general-purpose medium of exchange (independent of any central bank), is secured by a mechanism known as cryptography and can be converted into legal-tender and vice versa" [1]. Cryptocurrency should not be confused with virtual currency which is a type of digital money that is usually controlled by its creators or developers. Cryptocurrencies work on a distributed public ledger called blockchain, which can be defined as a transactional database. Blockchain is a particular type or subset of so-called distributed ledger technology ("DLT"). DLT is a way of recording and sharing data across multiple data stores (also known as ledgers), which each has the exact same data records and are collectively maintained and controlled by a distributed network of computer servers, which are called nodes. A cryptocurrency wallet is a software program that allows the users to interact with the blockchain to control the balance of their cryptocurrencies and to send or receive cryptocurrencies [2]. Transaction IDs are unique identifiers of transactions which can identify a particular transaction made between users of the currency and therefore an important forensic artefact.

Cryptocurrency is technical and financial innovation, that becomes more popular every day, and because of that, it is no surprise that more criminals are using cryptocurrency. According to a study conducted in 2020, there has been a shift from Bitcoin to privacy-oriented cryptocurrencies in the dark web markets [3]. Across all cryptocurrencies tracked by Chainalysis total transaction volume grew to $15.8 trillion in 2021, up 567% from 2020's totals. According to the report of Chainanalys, there is the huge increase in criminal balances in 2021 — at the year's end, criminals held $11 billion worth of funds with known illicit sources, compared to just $3 billion at the end of 2020. Also, there is mention of how much stolen funds dominate, as of the end of 2021, stolen funds account for 93% of all criminal balances at $9.8 billion. Darknet market funds are next at $448 million, followed by scams at $192 million, fraud shops at $66 million, and ransomware at $30 million. Criminal balances also fluctuated throughout the year, from a low of $6.6 billion in July to a high of $14.8 billion in October [4].

The criminal use of cryptocurrency is no longer confined to cybercrime activities, but now relates to all types of crime that require the transmission of monetary value. All criminals have one common goal for using cryptocurrencies - to keep their non-legal funds safe from authorities. Public-oriented cryptocurrencies do not satisfy that goal, because any transaction on a blockchain is transparent, visible to those who have access to it, and all transaction details are traceable. Contrastingly, with private-oriented cryptocurrencies all the transactions are hidden, and no one except transaction parties can view them, and transaction details are cryptographically protected and untraceable. Public cryptocurrencies are slowly, but surely losing their popularity in favor of private-oriented cryptocurrencies. Bitcoin is the most widely used and popular cryptocurrency [5], consequently, many studies and research on forensic analysis about Bitcoin and its blockchain have been carried out. On the other hand, research on privacy-oriented cryptocurrencies is not very common, and we found few studies related to the analysis of them. One of these studies is focused on the forensic analysis of Monero and Verge [6], while the other one is focused on the forensic analysis of Zcash and Dash [7].

The aim of this paper is to give a brief summary of the private-oriented cryptocurrencies – Monero, Verge, Dash, and Zcash, from a forensics perspective. There are three forensic investigations for uncovering (transactions with) private-oriented cryptocurrencies: blockchain, network, and wallet. Blockchains are publicly visible to everyone, and the forensic investigator can most easily access the information in them. Therefore, our focus in this paper is to overview why successful blockchain investigation is almost impossible. In Section 2 we explain technologies with which are provided anonymity and privacy, and tracing solutions. Section 3 presents three types of investigation. First type is already mentioned blockchain forensics. The next type of investigation is network investigation, but it also is not forensically helpful. Wallet investigation is the most useful because the most useful forensic artifacts related to transactions can be found. But this type is also the most unreal, because the chances are very small that the forensic investigation will gain access to the criminal's wallet. More detailed analysis for Monero, Verge, Dash and Zcash investigation is given on Section 4. At the end we give some conclusion.

2. Privacy-oriented cryptocurrencies and tracing solutions

The forensics investigator must have technical knowledge for the technology under review, therefore we describe how popular private-oriented cryptocurrencies work, how provide privacy and anonymity, which are forensics challenges, and what type of information can be found on the blockchain. Once the investigator achieves obtaining the transaction ID, this can be used to gather more information regarding the transaction on the blockchain.

Monero

Monero is a private, decentralized cryptocurrency, and as they claim it cannot be traced. Monero was launched in April 2014, as a fair, pre-announced launch of the CryptoNote reference code. Monero technology stands for Security, Privacy, and Decentralization. Since every transaction is private, that is a great forensic challenge, because the sender, receiver, and amount of

every single transaction are hidden. Monero uses three important technologies: Stealth Addresses, Ring Signatures, and RingCT [8].

The Stealth Address has underlying address info of two public keys, and a one-time public key is used as a transaction destination, to protect the recipient's privacy. Monero's Stealth Addresses are the concatenation of a public spend key and a public view key. The Stealth Addresses allow and require creating random one-time addresses. For creating a unique one-time address, a Diffie-Hellman-like exchange is applied to the user's address, for each transaction output to be paid to the user. Even external observers who know all users' addresses cannot use them to identify which user owns any given transaction output [9-11].

Ring signatures used in Monero are created from a combination of the sender's account key with a number of public keys, using a triangular distribution. This makes them private, because the identity of the sender is hidden, as it is computationally impossible to determine which of the group members' keys was used to produce the complex signature. In a "ring" of possible signers, all ring members are equal and valid. Furthermore, there are no fungibility issues with Monero given that every transaction output has plausible deniability (e.g., the network cannot tell which outputs are spent or unspent) [12].

Ring Confidential Transactions (RingCT) is an extension of CryptoNote protocol, and allows the amounts sent in a transaction to be hidden. The Ring Confidential Transactions protocol provides a strongly decentralized cryptocurrency (i.e., there is no privileged party) that has provable security estimates regarding the hiding of amounts, origins, and destinations. In addition, coin generation in the Ring Confidential Transactions protocol is trustless and verifiably secure [13].

Therefore, we described technologies used in Monero for providing security, privacy, and anonymity. We can suppose that Monero's claim for untracibility is correct, and that can be a huge forensic challenge. But Monero is not untraceable, as they claim. CipherTrace announced Monero Tracing solution. CipherTrace takes Monero tracing capabilities to the next level with the ability to follow the flow of funds backwards from the transaction of interest to its source [14]. However, Monero transactions are cryptographically secure using the latest and most resilient encryption tools available, and because of that, it is still a huge forensic challenge.

Verge

Verge is a multi-algorithm enabled proof-of-work based cryptocurrency, it is one of the few cryptocurrencies to support five hash functions combined on one blockchain. Verge was created to bring tailored transactional applications and inherent privacy implementations to strengthen user obfuscation. Verge creators believe that every person deserves the right to privacy and with that idea in mind, they pride themselves on being able to provide several different available methods of transacting across the Verge network. Each method provides users with a base level of obfuscation through the TOR network as well as different obfuscation options tailored for everyone's specific needs. TOR's use is intended to protect the personal privacy of users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities from being monitored. In short, when a user connects into the TOR network, their internet traffic is then routed through several global servers, each of which removes information from the previous server such that the last exit node server ends up being clueless as to where the network originated from. Verge has three types of transactions: simple, stealth, and anon [15].

Anyone can see the balance and simple transactions of any Verge address. Verge addresses are not themselves linked to a person or entity and users remain pseudo-anonymous so long as different addresses are used per transaction and or until the information is revealed during a purchase or other transactional circumstance [15]. This transaction works just like Bitcoin, so it is not a huge forensics challenge.

Stealth transactions are primarily compromised by dual-key stealth addresses, which are a method by which additional obfuscation can be implemented to further protect the receiving party when transacting with Verge. Stealth Addressing allows senders to create an unlimited number of one-time destinations addresses on behalf of the recipient without any interaction between the parties. When multiple users send funds to a stealth address, rather than these transactions appearing on the blockchain as multiple payments to the same address, they instead appear as multiple payments going to different addresses [15]. This makes it near-impossible to link transactions to the recipient's published address or one-time generated addresses. That type of transaction is a forensic challenge because it is designed such that the recipients are protected and can maintain their privacy, although stealth addresses do not provide anonymity and do not protect the sender.

Anon transactions use a combination of dual-key stealth addresses and RingCT to preserve the anonymity of both the sending and receiving parties. Ring Signatures make it harder to trace transactions by obscuring the output of the true sender in a set of other outputs on the blockchain, confidential transactions hide the actual amounts being sent, and TOR hides both parties true IP addresses i.e., IP obfuscation [15]. That type of transaction is a huge forensic challenge because it is designed for those who are fully looking to maintain their personal privacy.

Dash

Dash is the first cryptocurrency based on Bitcoin, with built-in privacy functions, it was launched in 2014. Dash aims to be the most user-friendly and scalable payments-focused cryptocurrency in the world. The Dash network features instant transaction confirmation, double spend protection, optional privacy equal to that of physical cash, a self-governing, self-funding model driven by incentivized full nodes, and a clear roadmap for on-chain scaling to up to 400MB blocks using custom-developed open-source hardware [16].

There are two main tiers: the miners and the master nodes. The miners carry out similar functions to those in the bitcoin network, so they are not a huge forensics challenge. Thanks to master nodes, which is an innovative two-tier network, Dash can offer innovative features in a trustless and decentralized way. Masternodes enable few services, but only CoinJoin makes a forensic challenge for investigating this type of tier. CoinJoin gives financial privacy through a decentralized implementation of CoinJoin [17]. The most notable privacy modification in Dash is its PrivateSend functionality. PrivateSend is a branded implementation of the CoinJoin protocol. When users take advantage of the PrivateSend function, the mixing is carried out for them and coins are deposited in new addresses. By the end of the process, the origin of the coins is obfuscated. PrivateSend is optional, and Dash transactions are unmixed by default. The general principle behind these mixing services is that multiple people send funds into one big transaction and each person receives the same amount of funds to a new address that they control. It then becomes difficult to connect each input to each output. For Dash's PrivateSend transactions, a user's funds are broken down into standard denominations: 10, 1, 0.1, 0.01, or 0.001 DASH. These funds are then sent in mixing transactions that only consist of that particular denomination. The user gets the same total amount of Dash back, but it's been mixed together with other PrivateSend users' funds. The outputs of these mixing transactions can then be sent in PrivateSend transactions to another user.[18]

According to Chainalysis, mixing transactions related to PrivateSend make up roughly 9% of all Dash transactions, and the percentage of Dash transactions that constitute actual transfers of funds using PrivateSend is less than 0.7%. Mixing transactions are very easy to spot and identify on the Dash blockchain. For the reason that they are still public and transparent, the same techniques

that can be used to analyze CoinJoin transactions performed using Bitcoin can be used on Dash. This means that while PrivateSend does increase privacy for its users, successful investigations can still be performed [19].

Zcash

Zcash is a privacy-protecting, digital currency built on strong science. Zcash was first released in October 2016, and it was originally based on Bitcoin's codebase. The Zerocash protocol is being developed into a full-fledged digital currency, Zcash. Zerocash extends the protocol and software underlying Bitcoin by adding new, privacy preserving payments. Zcash has its unique advantage. Zcash's anonymity relies on a shielded pool, where partial transaction information such as input/output addresses and the transaction value are no longer directly available from the Blockchain. Zcash is a cryptocurrency that uses advanced applied cryptography to provide enhanced privacy via shielded addresses. Zcash is the first practical application of zk-SNARKs [20], a specific type of zero-knowledge proof, a novel form of zero-knowledge cryptography.

Zcash addresses are either shielded (z-addresses) or transparent (t-addresses). Z addresses are private addresses and only the user can see the balance in the wallet. Shielded addresses are the address type that use zero-knowledge proofs to allow transaction data to be encrypted but remain verifiable by network nodes [21]. Senders to a shielded address may or may not include an encrypted memo. Transparent addresses work similarly to Bitcoin addresses and do not offer privacy for users [21].

Zcash has four basic types of transaction: transparent/public transaction (t-address to t-address), shielding transaction (t-address to z-address), de-shielding transaction (z-address to t-address), and shielded/private transaction (z-address to z-address). In a transparent transaction all transaction details are public (value is revealed by both sender and receiver). This transaction works just like Bitcoin, so it is not a huge forensics challenge. In shielding transaction t address and its sending amount are public, z address is encrypted. In de-shielding transactions t address and the amount, it receives are public, and the z-address is encrypted. Recipients of a shielded or de-shielding transaction do not learn about the sender's address through the transaction receipt in their wallet. The receivers only learn the value sent to their address(es) and if receiving to shielded addresses, any encrypted memo that may have been included by the sender [21]. Finally, in the most secure shielded/private transactions the addresses, transaction amount, and the memo field are all encrypted and not publicly visible. Encryption is the main forensics challenge, so only the shielded/private transactions are a forensics problem.

The Chainalysis solution can trace 99% of transactions. According to Chainalysis, roughly 14% of Zcash transactions involve one of Zcash's two shielded pools in some way. But of the transactions that interact with a shielded pool, only 6% are completely shielded, i.e., sender, receiver, and transaction amount are all encrypted. That's only 0.9% of all Zcash transactions. So even though the obfuscation on Zcash is stronger due to the zk-SNARK encryption, Chainalysis can still provide the transaction value and at least one address for over 99% of ZEC activity [19].

3. Types of investigations of the private-oriented cryptocurrencies

Blockchain investigation

Monero is the only cryptocurrency that has only private transactions, while in other cryptocurrencies privacy and anonymity are provided by a choice, not by default. Public transactions are identical to transactions with public cryptocurrencies, so all (forensic valuable) information can be found on the blockchain. With Zcash shielding and de-shielding transactions, parts of information can be found on the blockchain, explained in Section 2. Private transactions with private-oriented cryptocurrencies when they are properly implemented, are hidden, and no one except transaction parties can view them, and transaction details are cryptographically protected.

Network investigation

All network traffic for all types of transactions is encrypted. As we have already said, encryption is a big forensic challenge, so it is almost impossible to discover useful forensic artifacts with a network investigation. DNS traffic is unencrypted, as required by the protocol, for Monero it's traffic from the OpenAlias mechanism that is based on DNS. In Monero transactions destination IP address is the donation public address of the Monero. IP addresses of Dash seeder or nodes are destinations IP addresses in Dash transactions. In Zcash transactions destination IP address is Amazon

Wallet investigation

The most useful type of investigation is because the most useful forensic artifacts can be found. The transaction ID and amount can be found in all wallets for all types of transactions. The wallet passphrase in Monero wallet can be found after the creation of it, in Verge wallet only when unlocking the wallet with the passphrase, while in Dash and Zcash cannot be found. On the sender's side, the recipient's public wallet address can be found in the Monero wallet, the recipient's stealth address with a corresponding linked public address or recipient's normal public address can be found in the Verge wallet, and the recipient's private/public address can be found in the Dash and Zcash wallets.

4. Forensics investigation for Monero, Verge, Dash and Zcash

According to the previous section, if the transaction was private, forensics investigators cannot find the valuable information on the blockchain. The blockchain will show only general information such as the date, the ID, and the fee. Forensics' valuable artefacts can be found on the wallet, so if the investigator succeeds in recovering, that would be good progress for the investigation. In this section we analyze the investigations made by W. Koerhuis, T. Kechadi, and N.-A. Le-Khac [6], and Juan Manuel Delgado García [7].

Monero

Monero claims that a Monero account, or wallet, stores the information necessary to send and receive Monero. In addition to sending and receiving, the Monero Wallet software keeps a private history of your transactions and allows you to cryptographically sign messages. It also includes Monero mining software and an address book [23]. The experiment done by W. Koerhuis, T. Kechadi, and N.-A. Le-Khac confirms Monero's claim. In their experiment, they created eight memory images: after the creation of the wallet, after unlocking the wallet, after receiving one transaction, after sending a transaction, after sending a transaction with a full payment id, after receiving a transaction with an integrated wallet address, after an OpenAlias resolve action, and after the closure of the wallet. They found a wallet passphrase in every image. It is valuable from a forensics perspective because with a wallet passphrase forensics investigator can gain full control over a wallet and all the funds inside. The public address of own wallet was found in seven images (except the first one), it is necessary information for receiving Monero. After the first transaction there was a transaction ID and amount. In the next images there was additionally a transaction(s) ID, which is a private history of transactions. This refers to necessary information for sending and finding a public receiving address. During the disk analysis, they found out only two files monero-wallet-gui.log and M0n3r0wall3t.address.txt (M0n3r0wall3t is the name of the wallet). The first file is a general log file, and forensics artefacts were the public address of own wallet, transaction IDs of all transactions, and amounts of XMR received and sent. The second file contains only the public address of the wallet. Also, they found an encrypted {wallet_name}.keys file, this file contains the private keys, and can

be decrypted with the passphrase. The passphrase was not found on the disk, but the memory image experiment revealed the passphrase so this file can be decrypted [6].

Verge

W. Koerhuis, T. Kechadi, and N.-A. Le-Khac during the Verge experiment discovered an interesting fact while sending a transaction to a stealth address. When a sender initiates a fund transfer to a stealth address, the sender's public one-time address is saved in the transaction information. This one-time public address is stored in the receiver's wallet and is viewable on the blockchain. The one-time public address can now be linked to the recipient, and if the receiver wants to spend the coins on that one-time public address, that transaction can also be linked. After accepting the transaction, the own linked normal public address to the corresponding linked public address was discovered [6].

Dash

Juan Manuel Delgado García did Dash experiments. In memory, the transaction ID was found under the keyword AddToWallet, but no more information regarding this one was shown. Only in the case with Instant Send showed some details regarding the transaction. In general, correlating the ID, sending address, and the amount would be difficult for the investigator since this information is dispersed when analyzing the memory file making no sense. In a case with Private Send in the memory file, the MFT records showed evidence that the file dash.exe has been used. Although this file is not a forensics artefact, it can tell the forensics investigator that there exists the probability that in the memory acquisition there is the mnemonic phare to restore the wallet and access the complete information this contains. If the wallet is encrypted the mnemonic phrase will not be present in the wallet.dat file, and this option can be discarded. Disk artefacts are useful since it is possible to see the addresses in the wallet.dat file. The debug.log did not offer many details other than the transaction ID. Network findings showed information limited to DNS queries due to the traffic being encrypted by the application [7].

Zcash

Juan Manuel Delgado García made Zcash experiments. After the download, installation of the wallet, and execution, the structured analysis showed information about Master File Table (MFT) record. Unstructured analysis showed information about the transparent and private addresses. During the structured analysis for shielded transactions, on the side of the receiver no valuable artefacts were found, on the side of the sender, the MFT record was shown of the creation of the file AddressBook.json, with a label given by the user with its corresponding shielded and transparent addresses. Unstructured analysis shows information about the incoming/outcoming transaction, the transaction ID, the sending/receiving shielded address, the amount, and the memo field in hexadecimal format. For the de-shielded transactions, the structured analysis did not show valuable information. Unstructured analysis on the side of the receiver showed the incoming transaction in JSON format, this includes the transaction ID, the destination transparent address, the amount, and the timestamp in UNIX format. On the other side, the unstructured analysis did not show the transaction in JSON format and showed only the transaction ID. Structured analysis for shielding transactions and transparent transactions on the side of the sender did not show relevant information, the unstructured analysis showed evidence of the transaction in JSON format. As information in the shielding transactions is given: the transaction ID, the amount, the fee, and the timestamp in UNIX format. And, in the transparent transactions are given the information: the fee, the amount, the recipient's transparent address, and the transaction ID. Transparent and shielded addresses from the local wallet were present in memory in all cases [7].

5. Conclusion

Blockchains are publicly visible to everyone, and the forensic investigator can most easily access the information in them. With public transactions, all transaction information is accessible in plaintext on a blockchain. While with the properly implemented private transaction the blockchain shows only general information such as the date, the ID, and the fee. Privacy and anonymity are provided in a variety of ways, but all use encryption which makes forensic investigation almost impossible. There are solutions for tracking transactions, but not for disclosing transaction information. All network traffic except the DNS traffic is encrypted, so network investigation can hardly be useful. Wallet investigation is the most useful, because there are many helpful forensic artifacts related to transactions. But this type is also the most unreal, because the chances are very small that the forensic investigation will gain access to the criminal's wallet.

References

1. R. Houben, A. Snyers, Cryptocurrencies and blockchain - Legal context and implications for financial crime, money laundering and tax evasion (2018)
2. Blockgeeks, Cryptocurrency Wallet Guide: A Step-By-Step Tutorial, available at https://blockgeeks.com/guides/cryptocurrency-wallet-guide/ (2020)
3. E. Silfversten, M. Favaro, L. Slapakova, S. Ishikawa, J. Liu, and A. Salas, Exploring the use of Zcash cryptocurrency for illicit or criminal purposes (2020)
4. Chainalysis, The 2022 Crypto Crime Report (2022)
5. Coinmarketcap charts, available at https://coinmarketcap.com/ (2022)
6. W. Koerhuis, T. Kechadi, and N.-A. Le-Khac, Forensic analysis of privacyoriented cryptocurrencies (2020)
7. J.M. Delgado García, Forensic Analysis of privacy-oriented cryptocurrency wallets (2021)
8. Monero, What is Monero (XMR)? available at https://www.getmonero.org/get-started/what-is-monero/
9. Monero, Moneropedia - Stealth Address, available at https://www.getmonero.org/resources/moneropedia/stealthaddess.html
10. B. El Khoury Seguias, Monero's Building Blocks - Stealth addresses (2018)
11. G. Yu, Blockchain Stealth Address Schemes (2020)
12. Monero, Moneropedia - Ring Signature, available at https://www.getmonero.org/resources/moneropedia/ringsignatures.html
13. S. Noether, A. Mackenzir, and Monero Core Team, Ring Confidential Transactions (2016)
14. CipherTrace, CipherTrace Announces Enhanced Monero Tracing Capabilities for Government Agencies and Financial Institutions, available at https://ciphertrace.com/enhanced-monero-tracing/
15. Official Verge Blackpaper 5th edition, available at https://vergecurrency.com/static/blackpaper/verge-blackpaper-v5.0.pdf
16. Dash Documentation, What is Dash? available at https://docs.dash.org/en/stable/introduction/about.html
17. Dash Whitepaper - Dash: A Payments-Focused Cryptocurrency (2021)
18. Dash Documentation, Features, available at https://docs.dash.org/en/stable/introduction/features.html
19. Chainalysis, Introducing Investigations & Compliance Support for Privacy Coins Dash and Zcash, available at https://blog.chainalysis.com/reports/introducing-investigations-compliance-support-for-privacy-coins/ (2020)
20. A. Banerjee, M. Clear, H. Tewari, Demystifying the Role of zk-SNARKs in Zcash (2020)
21. Zcash Documentation, Addresses and Value Pools in Zcash, available at https://zcash.readthedocs.io/en/latest/rtd_pages/addresses.html