A Survey on Monero and ZCash

Alekhya Velicheti
MENG – Information Systems Security
Concordia University
Montreal, Canada
alekhyavelicheti99@gmail.com

Amukthamalyada Vellanki
MENG – Information Systems Security
Concordia University
Montreal, Canada
vamukthamalyada@gmail.com

Gurumurthy Anagandhula
MENG – Information Systems Security
Concordia University
Montreal, Canada
guruanagandhula123@gmail.com

Lakshmi Vintha
MENG – Information Systems Security
Concordia University
Montreal, Canada
lakshmivintha26@gmail.com

Shankar Teja Yalavarthy
MENG – Information Systems Security
Concordia University
Montreal, Canada
yalavarthy.shankar@gmail.com

Yashwanth Reddy Bandaru
MENG – Information Systems Security
Concordia University
Montreal, Canada
yashwanthr789@gmail.com

Abstract- **Monero and ZCash are the two most popular cryptocurrencies that put a priority on user anonymity and security, which emphasizes privacy. In this Project, we have analyzed and evaluated these two privacy-focused cryptocurrencies. The project focuses on a detailed understanding of each protocol's operation and highlights its strengths and weakness. We have analysed recent attacks that have been discussed at significant security conferences and given an in-depth understanding of the privacy and security attributes of these two cryptocurrencies and any possible flaws.**

Despite the fact that these two cryptocurrencies take distinct approaches to privacy, they both offer perks and drawbacks. In this project, we have studied attacks and delved into the technical details of these protocols in order to evaluate the benefits and drawbacks of various cryptocurrencies.

Recent cryptocurrency hacks have brought attention to the necessity of ongoing vigilance and fast upgrades to ensure their security and privacy. The thorough examination of these cryptocurrencies, their protocols, and current assaults presented by this project will be useful in determining their potential vulnerabilities and the effectiveness of their privacy features.

I. INTRODUCTION

Cryptography is a approach used to secure and authenticate transactions as well as control the generation of new units in the virtual currency known as cryptocurrency. Bitcoin is the original and utmost well- known cryptocurrency. It operates independently of a central bank or other financial institution and keeps track of all transactions via the blockchain, a decentralized database. [1]

Monero and ZCash, examples of cryptocurrency, resemble bitcoin in many aspects but have more privacy features. Both cryptocurrencies provide advanced privacy features that let users maintain the secrecy of their transactions. The approach to privacy is different for both cryptocurrencies, and this affects their level of security.

In recent years, assaults have been made against both Monero and ZCash. In 2021, researchers identified a vulnerability in Monero's ring signature, the attack happened in 2020, and a flaw in the RingCT protocol used by Monero was found that made it possible for an attacker to produce fake transaction outputs. Thanks to a network upgrade, this attempt was thwarted. The zk-SNARKS protocol used by ZCash was found to have a vulnerability in 2021 that may be used by an attacker to produce fake proofs. A network upgrade also patched this issue.

The attacks on Monero and ZCash show how constant monitoring and security maintenance are required in the cryptocurrency industry. To maintain the security and privacy of these cryptocurrencies, it is critical for both users and developers to be informed about potential vulnerabilities and to deploy effective mitigation techniques. The ongoing monitoring and timely improvements required to ensure the security and privacy of these cryptocurrencies are highlighted by these attacks. Thus, it is important to understand the concept of Monero and ZCash in detail. [2]

II. WORKING OF MONERO AND ZCASH PROTOCOLS

A. Monero

A cryptocurrency with a privacy focus termed Monero employs a number of methods to provide its users' anonymity. To secure users' anonymity, the Monero protocol makes use of a number of elements, including ring signatures, stealth addresses, and secret transactions. [18]

Ring Signatures: The Monero protocol makes use of ring signatures to mask the sender's identity. A ring signature is a type of digital signature that enables a user to sign a communication secretly. In Monero, ring signatures are used to construct a collection of prospective senders known as a ring, from which it is impossible to identify the real sender. [20]

Stealth Addresses: To conceal the identity of the recipient, Monero uses stealth addresses. Each transaction generates a unique public address called a stealth address. Money sent in Monero to a recipient's stealth address is immediately sent to the recipient's real address, which is kept secret from the general public. [20]

The Monero protocol also makes use of secret transactions to obfuscate the amount of Monero being transmitted. Only the sender and recipient have access to the real amount transmitted in a secret transaction since it is encrypted. Because of this, no one else can determine how much Monero is being exchanged.

RingCT: RingCT, an expansion of the ring signature and secret transaction protocols, was introduced by Monero in 2017. RingCT enables the concealment of both the sending amount and the sender's identity. It accomplishes this by generating a special range proof for each transaction that establishes the transaction's positive value without disclosing the precise amount. [20]

Mining: To verify transactions and create new coins, Monero employs the Proof of Work (PoW) consensus algorithm RandomX. ASIC-resistant RandomX makes it challenging to develop specialized hardware for Monero mining. This makes it possible for mining to continue being open and decentralized. [20]

B. ZCash

The ZCash protocol uses a particular technology called zk-SNARKs to enable transactions to be private. Transparent and protected transactions are made possible by this technology. Transparent transactions are like regular cryptocurrency transactions in that the blockchain can see them. On the other hand, shielded transactions rely on zk-SNARKs proofs to keep the sender and recipient's identities and the transaction amount secret. They are private.

The sender creates the transaction using their private key and encrypts it using the recipient's public key when a shielded transaction is initiated. A zk-SNARKs proof of the transaction is included to confirm its legitimacy and the sender's availability of funds. The transaction is added to the blockchain and the money is sent after the recipient decrypts the transaction with their own private key and validates the evidence using the public parameters.

Additionally, the ZCash protocol includes a special function called "Selective Disclosure" that lets users choose to reveal particular details about their transactions. When a person wants to establish ownership of money while preserving their anonymity, this capacity may prove useful. [3]

III. ATTACK SCENARIOS AND COUNTERMEASURES

Using anonymity overlay networks like Tor [4] or mix networks like Loopix [5] is a common mitigation for deanonymization attacks based on network analysis.

Tor helps to hide the connection between the originating node's IP address and the first node to broadcast the transaction to the peer-to-peer network, but we cluster transactions based on the entry nodes of the first broadcaster rather than the originating node's IP address. Keep in mind that broadcasting transactions through Tor can even lead to further man-in-the-middle vulnerabilities. [6]

Depending on the style of the user's wallet, we separate the scenarios into three categories.

1. Full node with incoming connections (server): A company or an enthusiast eager to volunteer their processing power to benefit the network typically runs a Bitcoin server. In the first scenario, numerous customers of this company may be involved in the transaction relayed through the

node, which is damaging to their privacy.

2. Full node without incoming connections: Depending on the collection of entry nodes, transactions coming from a complete node that has no incoming connections may be clustered. The user can restart the software after completing a transaction to avoid this so that each transaction is broadcast across a fresh set of entry nodes.

3. Light wallets: The majority of Bitcoin users employ lite wallets, or minimal payment verification, to outsource validation to another complete node (SPV). Most light wallets, especially ones that are portable, do not even connect to a P2P network from a networking perspective. Instead, they submit transactions over TLS to the server of the wallet provider and broadcast them to the P2P network.

The final phase of an anonymous transaction is when a wallet processes new transactions, and this is where we found the most applicable and widespread side-channel attacks. The unlikability and anonymity guarantees of the system can be violated by remote adversaries using these attacks.

A. Attack Type I: Side-Channels at the Receiving Party

Attacks like cache side-channel attacks could be used by an adversary co-located with a user's wallet. Such adversaries, however, are expressly excluded from the threat model taken into account by Monero and ZCash. [7]

The goals of the attacker include figuring out whether two transactions pay the same address and how a known user connects to the P2P network.

We take into account two distinct assault scenarios: To find out which P2P node (or wallet) the key's owner uses to accept transactions, the adversary knows an anonymous public key and sends a transaction to it. An honest user sends a transaction for which the intended payee's public key and identity are unknown to the adversary. Which P2P node (or wallet) is utilized by the transaction's payee is determined by the opponent.

Because the attacker can transmit legally designed transactions to a known public key, the latter attack scenario incorporates the first. A break in transaction unlikability results straight from the second case. The attacker only must know if the payees of two transactions that have been sent into the network share the same P2P node or wallet. Both attack scenarios also compromise user anonymity and can be leveraged for further privacy violations:

1. IP address recovery. If the owner doesn't utilize anonymizing software like Tor, the adversary can connect a public key to the IP address of her P2P node (or her wallet if it connects to a remote node). The victim can be geo-localized or de-anonymized using this information.

2. Diversified address linkability. An attacker can identify whether two public keys are for the same user if they are given two public keys. The attacker attempts to identify the same node or wallet by sending a transaction to each public key. The unlinkability feature of varied addresses is violated by this.

3. Private key recovery. The flaws in several of our assaults also provide opportunities for side-channel timing extraction of a victim's secret "viewing" key. If this key is stolen, the attacker can link all transactions sent to the victim passively (but not take money from the victim).

B. Attack strategies.

Strategy 1: Analyzing wallet-to-node communication traffic. A network adversary or remote node adversary can passively watch changes in the wallet-to-node interaction if a wallet connects to a distant node.

Strategy 2: Wallet behavior can be inferred from the P2P layer. Co-locating the wallet and node prevents a remote adversary from watching how they interact. Yet, information still leaks to the adversary if changes in wallet behaviour affect how the user's P2P node communicates with distant peers.

Both approaches function when a transaction is made, sent into the P2P network, and when it is part of a block. Wallets then reprocess the transactions to make sure they are genuine (i.e., they did not double-spend), and the block and all of its transactions are then shared with each peer.

C. Attack Type II: Side-Channels at the Sending Party

This section includes more conceptual criticisms. These attacks, however less likely to affect present users, serve as a reminder of the significance of having side-channel-free cryptographic implementations for the long-term and comprehensive security of anonymity-preserving systems.

Attack strategy: We take into consideration a cryptographic timing attack that takes the use of temporal variations in arithmetic operations based on the values of the operands. Prior to this study, such attacks for many cryptographic primitives have not been taken into account for zk-SNARKs. We take advantage of the correlation between the length of the proof's production and the significance of the prover's witness. We anticipate that the transaction amount, which is contained in the witness, will be tied to the duration of the proof. In the proofs for ZCash, for instance, the transaction amount is divided into bits, and for each non-zero bit, an elliptic curve operation is computed. Hence, the transaction amount's Hamming weight, which is connected with its value, and the proof time are both highly correlated. [8][9][10]

D. The Transaction Flooding Attack

This attack analyses the ring signature mechanism of Monero, which hides the genuine input keys by combining them with various output keys (used as decoy keys) produced by earlier transactions. The transaction flooding attack's fundamental concept is straightforward. A large knowledge base, or set of output keys, must be accumulated by the attacker in order for the system to choose keys to be utilized as mix-ins in upcoming transactions. In order to establish an input ring of size 11 in Monero, each input must have 10 mixins in addition to the real spend key for each new transaction. The system adds the mixins to the transaction's input after selecting them from the output keys of earlier transactions using a decoy picker that makes use of a gamma distribution. [11]

E. The Attacker Model

The attacker can obtain blockchain data since Monero's blockchain data is open to the public and available to anybody. In order to be able to track transaction inputs, we presume that the attacker is prepared to pay transaction costs. In order to flood the network, we also assume that the attacker has access to at least two separate Monero addresses. The quantity of XMR required to cover the fees paid for the attack transactions must be present at one of those addresses. The other addresses will be used to store output keys and accept transactions. Remember that creating a new Monero wallet is easy and cost-free. Last but not least, we assume that the attacker can start as many transactions as he wants at any one moment, provided he pays the transaction charges. As there is no assurance of timing, it is up to the miners to select and approve the transactions. If the network's transaction pool contains transactions that are awaiting confirmation that pay higher fees, the miners will choose those first.

IV. SIMILARITIES AND DIFFERENCES BETWEEN MONERO AND ZCASH

A. Purpose

The protection of users' identities is the aim of private transactions. Some individuals think it is their right to spend their money in a covert, clandestine manner. In ZCash, the sender can choose whether to make these transactions public or private upon request. [12], Nevertheless, with Monero, all transactions are completely secret. [13]

B. Speed

The block time on the Monero blockchain is 2 minutes. According to this, new blocks are made every two minutes. This makes it around five times faster to transact with than Bitcoin.

The block time for ZCash is around 2.5 minutes. [14] This makes it somewhat slower than Monero and around four times quicker than Bitcoin for transactions.

Its speed with the ZCash blockchain is dependent on how active the network is. Your transaction might not appear in the first block if several other users are sending transactions at the same time as you. It can take a few blocks until it is incorporated. It is also important to note that each block has significantly more space due to private transactions. The network would conduct about six transactions per second if only private transactions were being processed. If no extra anonymity is employed by the transactions filling the block, this corresponds to a little over 26 transactions per second. [15]

This is not exactly how Monero operates. A dynamic block size cap exists. It follows that the blocks change in size in accordance with the network's demand. Each block's size is determined by the size of the 100 blocks before it. Thus, if a network is handling a large number of transactions, the block size will gradually rise, increasing the network's capacity. According to some sources that we have taken as references, Monero can process 1,700 transactions per second. This, however, has never even been remotely put to the test. [13]

C. Usage

These two privacy-focused programmes have different levels of usage, which is one area where they diverge. Compared to ZCash, Monero appears to be more popular on the dark web. This is because Monero is currently considerably more user-friendly than ZCash. Currently, there aren't many trustworthy wallets for the currency. Being a relatively new coin, this will undoubtedly evolve. [14]

On the dark web, rogue nations like North Korea that wish to circumvent international sanctions and hacking organizations have all found uses for Monero. [16] There are also more fascinating uses as a result of how easily it can be mined by conventional computer systems.

The reality that ZCash transactions are not required to be secret is one way why ZCash may edge out Monero in the battle of privacy currencies. This may assist businesses in staying compliant with "know your customer" laws in different nations and help them avoid any future regulatory troubles. [17]

D. In-Browser Mining and Crypto-Jacking

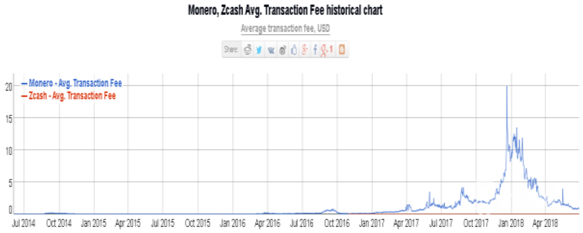
In-browser mining has become another use for Monero. This is due to the fact that Monero may still be mined with simply a GPU or CPU. Using mining software from an internet browser is known as "in-browser mining." Although incredibly simple to accomplish, it is not particularly effective. But it may be quite profitable if you can persuade hundreds or thousands of computer users to spend their power to do it for you. [18][19]

E. Crypto-Jacking

The fact that certain publications are compelling customers to mine cryptocurrencies for them is not always disclosed. Also, the files that consumers download from some download portals may include concealed Monero mining software. Crypto-jacking is when mining software is installed on a system without the owner's consent. Monero is chosen for crypto-jacking when ZCash VS Monero is compared due to its anonymous features and the fact that it is still mineable utilizing CPUs and GPUs. [12][13]

F. Cost of Fees

The typical Monero cost is now approximately 90 cents. Regarding the cost of Monero, this has drastically altered. The price to transfer Monero reached a high of a little over $20! The same scaling problems affect Monero as they do Bitcoin. [15] The typical ZCash charge is very minimal in contrast. Just 0.0001 ZEC is involved. Currently, this is less than 2 cents! They have stayed quite low during ZCash's existence, according to Bitinfocharts.com. [15]



G. Scalability

Monero's configurable block size restriction is an attempt to address scalability problems. This is insufficient to enable the network to be utilized by everyone on the earth, as seen by the enormous costs it has previously faced. [13]

ZCash, meanwhile, has more serious scalability problems than Bitcoin. If everyone wanted to create anonymous transactions, there would be a race to the top in transaction costs as secret transactions take up a lot of space in blocks than Bitcoin. In the spring of 2017, Bitcoin experienced this. Yet now, there isn't enough interest in ZCash for such a race to take place. [12]

H. Open-Source

Both Monero and ZCash are open-sourced cryptocurrencies, meaning that anybody can access, alter, and contribute to the network's source code. This transparency and confidence in the network are aided by this openness. [12][13]

I. Teams

The Monero team is mostly concealed from the public. The project's two principal developers are well-known. The others go under other names. The ZCash crew, however, is far more approachable. [18][19][12][13]

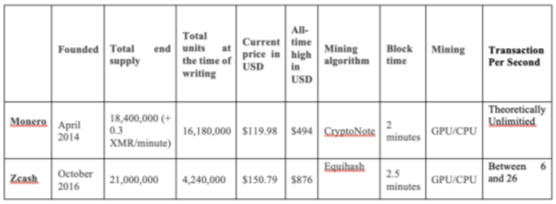
J. Market History

In 2014's infamous crypto bear market (a market that was gloomy), Monero was initially developed. The price movement versus the dollar was stable in its early years. No significant steps were taken in either direction. In the second half of 2016, when the whole cryptocurrency market began to turn optimistic, Monero also started to see an upward trend. As 2017 went on, this accelerated, and by the halfway point of the year, Monero, like the majority of other digital assets, saw a spectacular increase. [14]

Early in 2018, the cost of a single Monero currency reached its high. The high peaks of Bitcoin and every other cryptocurrency were met with this. Monero's all-time high price per coin was almost $500.The trend since this peak has primarily been downward with a few "bull traps" along the way. A Monero currency is now valued at around $120 as of the date of this writing (June 29, 2018). [15][12][13]

The price development of ZCash has a similar trend to that of Monero (and many other cryptocurrencies for that matter). The picture below shows that following its introduction, there was sideways price movement. Yet, the rise began a bit later than Monero's. [15]

The price started to increase in proportion to the US dollar in the middle of 2017. ZCash grew in value along with Bitcoin. ZCash declined at the same time as Bitcoin. Because of this, the orange line showing ZCash's performance relative to Bitcoin has essentially remained flat during the coin's existence. [18][19] Below is the picture of the comparison map between ZCash and Monero.



	Founded	Total end supply	Total units at the time of writing	Current price in USD	All-time high in USD	Mining algorithm	Block time	Mining	Transaction Per Second
Monero	April 2014	18,400,000 (+ 0.3 XMR/minute)	16,180,000	$119.98	$494	CryptoNote	2 minutes	GPU/CPU	Theoretically Unlimitied
Zcash	October 2016	21,000,000	4,240,000	$150.79	$876	Equihash	2.5 minutes	GPU/CPU	Between 6 and 26

V. CONCLUSION

There are so many cryptocurrency projects out there, even in the field of privacy coins, that it is overwhelming. And privacy coins are the clearest example of this. With ZCash and Dash as its major rivals, Monero is expected to maintain its position as the leading privacy currency. Compared to both combined, Monero presently has a bigger market cap.

New competitors in the privacy currency market include Tornado Cash and Pirate Chain, with the former providing superior protection against Sybil assaults. Investors should consider the possibility of competitive hash-rate takeovers affecting Monero itself.

When considering attacks on both Monero and ZCash there are two types of attacks they are Side-Channels at the Receiving Party and Side-Channels at the Sending Party, out of these two types of attacks on receiving party is the worst.

We have surveyed the potential side-channel attacks on wallet processing as well as attack scenarios on cryptocurrency anonymous transactions. Moreover, we recommend defenses employing anonymity overlay networks and side-channel-free cryptography implementations.

REFERENCES

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

[2] A. Biryukov, D. Khovratovich, and I. Pustogarov, “Deanonymisation of clients in Bitcoin P2P network,” in ACM Conference on Computer and Communications Security. ACM, 2014, pp. 15–29, https://arxiv.org/abs/1405.7418.

[3] Nir Bitansky, Ran Canetti, Alessandro Chiesa, and Eran Tromer. From extractable collision resistance to succinct non-interactive arguments of knowledge, and back again. In Innovations in Theoretical Computer Science 2012, Cambridge, MA,

USA, January 8-10, 2012, pages 326– 349, 2012.

[4] “Tor,” 2019, https://www.torproject.org/

[5] M. Piotrowska, J. Hayes, T. Elahi, S. Meiser, and G. Danezis,“The Loopix anonymity system,” in 26th USENIX Security Symposium(USENIXSecurity 17). Vancouver, BC: USENIX Association, 2017, p. 1199–1216. [Online]. Available :https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/piotrowska

[6] Biryukov and I. Pustogarov, “Bitcoin over Tor isn’t a good idea,” in IEEE Symposium on Security and Privacy. IEEE Computer Society, 2015, pp. 122–134, https://arxiv.org/abs/1410.6079

[7] Electric Coin Company. Zcash documentation|security warnings|side-channel attacks.https://zcash:readthedocs:io/en/latest/rtd pages/security warnings:html#side-channel-attacks, 2019. Revision fe830a5a.

[8] Paul C Kocher. Timing attacks on implementations of Di e-Hellman, RSA, DSS, and other systems. In Annual International Cryptology Conference, pages 104{113. Springer, 1996.

[9] David Brumley and Dan Boneh. Remote timing attacks are practical. Computer Networks, 48(5):701{716, 2005.

[10] Billy Bob Brumley and Nicola Tuveri. Remote timing attacks are still practical. In European Symposium on Research in Computer Security, pages 355{371. Springer, 2011.

[11] K. M. Alonso, “Zero to monero,” 2020.

[12] https://en.wikipedia.org/wiki/Zcash

[13] https://en.wikipedia.org/wiki/Monero

[14] J. -H. Lee, "Rise of Anonymous Cryptocurrencies: Brief Introduction," in IEEE Consumer Electronics Magazine, vol. 8, no. 5, pp. 20-25, 1 Sept. 2019, doi: 10.1109/MCE.2019.2923927.

[15] Bitinfocharts.com.

[16] A. Biryukov and S. Tikhomirov, "Deanonymization and Linkability of Cryptocurrency Transactions Based on Network Analysis," 2019 IEEE European Symposium on Security and Privacy (EuroS&P), Stockholm, Sweden, 2019, pp. 172-184, doi: 10.1109/EuroSP.2019.00022.

[17] A. Averin, A. Samartsev and N. Sachenko, "Review of Methods for Ensuring Anonymity and De-Anonymization in Blockchain," 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), Yaroslavl, Russia, 2020, pp. 82-87, doi: 10.1109/ITQMIS51053.2020.9322974.

[18] “Monero. private digital currency,” 2018, https://getmonero.org/.

[19] https://z.cash

[20] Monero:The secure, private, untraceable currency - https://getmonero.org/library/ZeroToMonero-1-0-0.pdf