A cryptographical comparison of Monero and Zcash

Ruben Biskupec[1]

Eindhoven University of Technology, The Netherlands
r.biskupec@student.tue.nl
https://www.tue.nl/en/

Abstract. In this paper I will discuss the context in which privacy coins were developed, their cryptographic protocols in use, thus their differences. Finally I will briefly look at possible attacks and countermeasures.

Keywords: Monero · Zcash · Ring signatures · zero-knowledge proofs · decentralized electronic cash.

1 Introduction

When Bitcoin [1] was released in 2009, it was thought to be almost untraceable. In 2011 Darknet markets like SilkRoad started to use this digital currency, paired with Tor, in order to sell illegal drugs anonymously. But it soon became clear that since the protocol has a transparent payment history on the blockchain, all transactions between addresses can be verified and therefore traced by any third party.

To mitigate this risk, mixer services [2] (also known as tumblers or laudries) like Bitcoin Fog or CoinJoin started to emerge, these work similarly to mixer networks and rely on a central third party. After transferring the coins, users must wait for a delay before withdrawing the coins from another address, so that the timing of incoming and outgoing transactions do not reveal their relationships. The other problems are the vulnerability to scams and tracing from the operator. Moreover, there is a risk of losing the funds if the mixer is seized while the funds are still locked. Finally, these services are expensive and complicated to use. Finally, newly minted coins become more valuable than coins linked to blacklisted transactions.

In 2013 researchers were able to prove that the identity of these addresses can be linked to real-world identities through clustering and heuristic techniques. [3] They even managed to track funds that went through mixing techniques all the way to the exchanges where it was withdrawn. Following this discovery, the company Chainalysis was founded, and it specializes in de-anonymizing techniques. As of now, it partners only with government law enforcement agencies like the FBI and Europol for investigating criminal activity [4] [5], but it means that

with the right tools, it is possible to de-anonymize anyone.

It is in this historical context that privacy enthusiasts, and criminals, had the need for an instant, risk-free, and secure digital currency that would not reveal their transaction history. Therefore, researchers began to work on possible solutions and anonymous cryptocurrencies started to emerge. In this paper, the 2 current leading privacy coins, Monero and Zcash, will be considered. I will compare their security properties and cryptographic implementations utilized to achieve the goals of anonymity on a public blockchain. At first, this might seem impossible to achieve, as the concept of a blockchain is that of publicly verifiable ownership. How can a miner verify transactions if the addresses and/or the amounts are hidden? We will demystify it in the following sections.

2 Monero

2.1 CryptoNote whitepaper

Monero is based on the CryptoNote whitepaper [6] from 2013. Its aim is to create an electronic currency with the properties of cash. In particular, it aims to solve unlinkability and untraceability. Over the course of the following years, the protocol evolved a lot and the documentation is not of the best quality, the codebase should be considered the only source of truth.

2.2 Unlikability: Stealth Address

Miners can censor transactions if they disagree with where the money is going by not including it in a block. To prevent this, all on-chain metadata must be obscured, as is done in Monero with the use of Stealth Addresses. Every user owns a dual-key, for example, the public keys of Alice (viewing and spending key) will look like this (K_A^v, K_A^s), corresponding to their private pair (tracking, spending)(k_A^v, k_A^s) When Alice wants to send 1 coin to Bob, an Elliptic Curve Diffie-Hellman key exchange is applied to create a one-time address for the transaction output. The process goes as follows:

Alice generates a random number $r \leftarrow Z$ and computes $K = H(rK_B^v)G + K_B^s$ [7] as the destination address. She then adds the amount '1' and the value $R = rG$ to the transaction, signs it with a one-time private key, and sends it into the network.

Bob will be checking every transaction to see if there is one destined for him. To do so, he calculates $k_B^v rG = rK_B^v$, then $K_B'^s = K - H(rK_B^v)G$ If $K_B'^s == K_B^s$ Bob knows that he is the target and is able to spend the money, but the address will look unlikable to him from an outside observer. This process makes syncing a wallet a much longer process than in blockchains like Bitcoin, but it is necessary to achieve privacy.

Bob can share his private tracking key with a third party (or make it public). Anyone who has access to it will be able to track which transactions belong to Bob, this can be useful for compliance. To prove that she sent the coin, Alice can either disclose r to Bob or use a zero-knowledge proof to prove she knows r to Bob. Most transactions will have many outputs to transfer back the change to the owner.

Subaddresses allow users to create an almost infinite number of addresses that are derived from a single main address, which acts as a seed. Each subaddress can receive Monero and all the funds are directed to the same wallet. This method enables users to operate a large number of identities under a single address while minimizing the amount of information that is exposed to the public. Additionally, these subaddresses are not mathematically linkable, meaning that it is difficult for an outside observer to connect them unless the user reveals the connection publicly.

2.3 Untraceability: Ring Signatures

To achieve untraceability, Monero implements a modification of the 'Traceable ring Signatures' [8] called one-time ring signatures. This variant is based on Curve25519 by D. J. Bernstein [9] and allows for double spend attempts to be linked together by the same signature.

These are a type of digital signature used to provide anonymity for transactions. It allows any member of an (improvised) group of users that have keys to perform a digital signature with a non-interactive zero-knowledge proof, even without their consent, making it computationally infeasible to determine which of the group members' keys was used to produce the signature.

These signatures are constructed by creating a ring of decoy outputs, which are real past outputs from the blockchain and have nothing to do with the present transaction. The size of the set of decoy outputs, plus the real one is called the ringsize. A larger ringsize improves privacy but increases the time and verification cost of the transaction, so it's important to find a balance between privacy and performance. Initially, a user could set a ringsize of 1, therefore revealing himself. This was later changed and now there is a mandatory ringsize of 11 provides plausible deniability by design. [36] There is a plan to raise this number to 16.

To avoid double spending, a key image (a unique one-time digital signature) is generated for each transaction by the sender and included in the blockchain. Miners verify that the key image was not already used so that no outputs can be spent twice.

It is worth noting that due to the fact that a ring signature could only combine outputs with the same value, transaction amounts need to be split into specific denominations. For example, a 12.5 Monero output would be divided into three outputs (three different ring signatures) of 10, 2, and 0.5 XMR in order to complete the transaction. [10]

The security guarantees of one-time ring signatures rely on the Discrete Logarithm problem being hard and are proved using the Random Oracle model. [6]

2.4 Concealing transaction amounts: RingCT

The original whitepaper did not include a way to hide transaction amounts, but the need to add such property arose. Gregory Maxwell had already developed Confidential Transactions (CT) as a way to hide transactions in Bitcoin. However, the proposition was not adopted. Monero was interested in using it, however, the technology of ring signatures was not compatible with CT. Shen Noether uses Multilayered Linkable Spontaneous Anonymous Group (MLSAG) to create Ring Confidential Transactions [11] (RingCT), which can be used with ring signatures. RingCT was introduced on the mainnet in 2017 and is mandatory for all transactions.

The cryptography involved is pretty advanced, but on a higher level it relies on the following:

Pedersen commitments . These are special kinds of commitments that hold a homomorphic property for addition. This relation is used to prove that the sum of the transaction's inputs equals the sum of the outputs, by encoding the exact amounts with a binding factor. Only the recipient can decode it and see the real amount.

Range proofs . The protocol needs to ensure that transaction outputs are not negative. (Otherwise, a user with 1 XMR could make a transaction sending 1000 XMR back to himself and -999 to a third party) These proofs demonstrate in zero-knowledge that the encrypted transaction amount is derived from the sum of positive numbers and is under an arbitrary upper limit (to prevent an overflow).

Thanks to RingCT, it is impossible for an outside observer to determine the exact amounts being sent, however, the miners are still able to validate the transactions and approve them. Also, transaction amounts can now be of any denomination. A problem still persisted, the proofs were big in size and took a long time to verify. For this reason, Bulletproofs [12] were added to Monero in 2018 for range proofs. Bulletproofs use Non-Interactive Zero Knowledge Proof

and do require a trusted setup. Under bulletproofs, transaction size scale logarithmically instead. The proof size was improved again with Bulletproofs+.

It is worth noting that the reward that miners get to generate the block is not hidden, this way the current amount of Monero in existence can be known publicly. Finally, the fee paid to the miners need to be public, so they can decide who to prioritize. [13]

3 Zcash

3.1 Zerocoin whitepaper

Zerocash can trace its origins to the Zerocoin whitepaper [14], which proposes a digital currency scheme that relies on non-interactive zero-knowledge signatures to achieve anonymity. It is not a complete cryptocurrency but rather a proof of concept extension of the Bitcoin protocol. Its use case would be for users to periodically wash their bitcoins. Its main limitations are the need for large proofs and slow verification times.

3.2 Zerocash whitepaper and zk-SNARKS

The Zerocash whitepaper [15] aims to solve those open problems and introduces even more privacy features. To achieve these goals it relies on the zero-knowledge Succinct Non-interactive ARguments of Knowledge (zk-SNARKs). [38] A SNARK is a succinct, complete, non-interactive, and knowledge sound proof that a certain statement is true. The proof pie must therefore be short and fast to verify (log(n)) and leak zero knowledge. [16] The mathematics is too complex to summarize here, but it is important to know that with this novel cryptographic primitive, the miners can verify the transactions and account balances without knowing the user's identity and transaction amount.

Similar to Monero, the sender of the Zcash transactions constructs a proof that states that the difference between the sum of the inputs and outputs is zero, the sender owns the private spending key, and the private key is linked to the transaction such that the transaction can not be altered without it. [10]

3.3 Zcash transaction types

The Zerocash whitepaper was then implemented by the Electric Coin Co. (ECC) as a fork of Bitcoin and was publicly launched in 2016 as Zcash. Currently, each user is assigned both a public (transparent) t-address and an anonymous z-address, which are interoperable. There are therefore 4 possible transaction types available [17]:

- Public. Similar to Bitcoin where all data is public.

- Shielding. The sender uses his t-address, while the receiver a z-address. The transaction amount will be known on the sender side, but hidden on the receivers.
- Deshielding. It is the opposite of a shielding transaction.
- Private. Both parties use their z-address and the transaction amount is kept secret.

The default is a public transaction while private transactions require the users to opt in. The main reason for this is performance, as generating proofs is computationally expensive.

3.4 Trusted setups

The main downside of zk-SNARKs is the requirement of a common reference string (CRS) for proving and verifying. The CRS needs to be generated in advance by a trusted third party and the information used to create it, called toxic waste, needs to be destroyed. Otherwise, an adversary could forge fraudulent proofs. In Zcash this would mean minting new coins out of thin air, but user privacy would be preserved. It is also worth mentioning that every time there is a hard fork, this ceremony needs to be repeated. [20]
The setup ceremony of choice is usually a Multi-Party Computation (MPC) [18], where the CRS is secure as long as at least one participant is honest. In Zcash's first ceremony, all participants needed to be available online for the whole duration of the protocol. This meant that for practical reasons only 6 people were involved.

Since then the aim has been to include the number of independent contributors, thus making collusion more complicated. In 2017 Bowe introduced a better way to perform these ceremonies. Since then the Powers of Tau became the standard to generate CRS and Zcash used it in 2018 with a total of 87 participants for a new hard fork. [19]

3.5 Trustless setups

Bowe later discovered Halo while working at the ECC [23], a new type of recursive (scalable) zero-knowledge proof that does not require a trusted setup which also allows for greater scalability [21]. Halo was implemented as Halo 2 [24] and was then introduced in Zcash in 2020, eliminating the risk of ceremony compromise. [22]

4 Attacks and countermeasures

4.1 Monero Linkability and Traceability

The main objections to Monero reside from the papers 'An Empirical Analysis of Linkability in the Monero Blockchain' [25] published in 2017 and 'An Empirical

Analysis of Traceability in the Monero Blockchain' [26] published a year later. Detailed responses from the developers can be found here [27] [28].
The key findings revolve around how zero-decoy and small ringsize transactions could be used to deanonymize users. Also, the algorithm that was used to pick the decoys had some flaws. The Monero team appreciated the critics and responded well, some of the vulnerabilities were already known and fixed, and the others were addressed later with the introduction of RingCT.

4.2 IPs and metadata

Zcash suffered an IP metadata leak from shielded addresses as described in this blog [29]. Monero can also suffer from similar problems. It is now recommended for both projects that the nodes use anonymity networks like Tor and I2P [30] or solutions like Dandelion [31].

4.3 Side-channel

Side-channel timing attacks were discovered in the paper 'Remote Side-Channel Attacks on Anonymous Transactions' [32]. The attacker would be able to identify the secret payee of a transaction in both Monero and Zcash. Finally, the time to generate a zero-knowledge proof depends on the amount of funds being transferred. Hence ad adversary capable of measuring this time could break confidentiality despite the zero-knowledge property. Both projects responded well to the findings and prioritized fixing the problems.

4.4 Sybil attacks

A motivated attacker could create many accounts to flood the blockchain with the hope of all of his addresses being included in a ring signature. He could then publish the private keys, thus revealing the identity of the true sender. [33] This could have been a problem when the ringsize was small, but it is now solved.

5 Conclusion

While Monero transactions are always anonymous, Zcash is only fully anonymous when sending between two z-address. The other thing to note is that Zcash is not private by default and only less than 5% of its transactions are shielded.[34] Some critics claim that this makes those transactions stand out. [40] The requirement of a trusted setup for its creation is also a security concern for some, but this is a solved problem now.

It is also worth noting that both are open source and are implementing some ASIC and GPU resistant hash functions, like CryptoNight [35] to maintain alive the philosophy of "one CPU, one vote". This makes them more decentralized than Bitcoin, which uses SHA-256.

Monero has more of a crypto-anarchist upbringing and has a more supportive community, while Zcash is owned by a company, has a CEO, and has links with both the Israeli and US governments. This makes criminals skeptical and is one of the reasons why Monero is the coin of choice in underground markets.

Moreover, there are no fungibility issues with Monero [39] given that every transaction output has plausible deniability, while it can be argued that the difference between t-addresses and z-addresses in Zcash makes the coins non-fungible.

I believe both projects are good options. In less than 10 years they were able to advance the state-of-the-art in cryptography. While it is true that some of the protocols in use are very new and they have not stood the test of time, they were audited by many researchers, and no vulnerabilities are known. In the end, deciding which one to use comes down to personal preference. Finally, we should be glad to have the option to choose because competition fosters innovation.

References

1. Nakamoto, S. and Bitcoin, A., 2008. A peer-to-peer electronic cash system. Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf, 4, p.2.
2. Möser, M., Böhme, R. and Breuker, D., 2013, September. An inquiry into money laundering tools in the Bitcoin ecosystem. In 2013 APWG eCrime researchers summit (pp. 1-14). Ieee.
3. Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCoy, D., Voelker, G.M. and Savage, S., 2013, October. A fistful of bitcoins: characterizing payments among men with no names. In Proceedings of the 2013 conference on Internet measurement conference (pp. 127-140).
4. Andy Greenberg, Wired, 2015, January. Prosecutors Trace $13.4M in Bitcoins From the Silk Road to Ulbricht's Laptop. URL: https://www.wired.com/2015/01/prosecutors-trace-13-4-million-bitcoins-silk-road-ulbrichts-laptop/
5. Department of Justice, 2021. U.S. Attorney Announces Historic $3.36 Billion Cryptocurrency Seizure And Conviction In Connection With Silk Road Dark Web Fraud. URL: https://www.justice.gov/usao-sdny/pr/us-attorney-announces-historic-336-billion-cryptocurrency-seizure-and-conviction
6. Van Saberhagen, N., 2013. CryptoNote v 2.0.
7. Alonso, K.M., 2020. Zero to monero.
8. Fujisaki, E. and Suzuki, K., 2007, April. Traceable ring signature. In International Workshop on Public Key Cryptography (pp. 181-200). Springer, Berlin, Heidelberg.
9. Bernstein, D.J., 2006, April. Curve25519: new Diffie-Hellman speed records. In International Workshop on Public Key Cryptography (pp. 207-228). Springer, Berlin, Heidelberg.
10. Stefan Stankovic, 2019. RingCT vs zk-SNARK: The Ultimate Guide to Monero and Zcash Privacy Mechanisms. URL: https://unblock.net/ringct-vs-zk-snark/
11. Noether, S. and Mackenzie, A., 2016. Ring confidential transactions. Ledger, 1, pp.1-18.

12. Bünz, B., Bootle, J., Boneh, D., Poelstra, A., Wuille, P. and Maxwell, G., 2018, May. Bulletproofs: Short proofs for confidential transactions and more. In 2018 IEEE symposium on security and privacy (SP) (pp. 315-334). IEEE.
13. Diego Salazar, 2020. How RingCT Hides Monero Transaction Amounts. URL: https://localmonero.co/knowledge/monero-ringct
14. Miers, I., Garman, C., Green, M. and Rubin, A.D., 2013, May. Zerocoin: Anonymous distributed e-cash from bitcoin. In 2013 IEEE Symposium on Security and Privacy (pp. 397-411). IEEE.
15. Sasson, E.B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E. and Virza, M., 2014, May. Zerocash: Decentralized anonymous payments from bitcoin. In 2014 IEEE symposium on security and privacy (pp. 459-474). IEEE.
16. Bitansky, N., Canetti, R., Chiesa, A., Goldwasser, S., Lin, H., Rubinstein, A. and Tromer, E., 2017. The hunting of the SNARK. Journal of Cryptology, 30(4), pp.989-1066.
17. Multiple transaction types. URL: https://z.cash/technology/
18. Anthony Mpho Matlala, Alex Pruden, 2021. Setup Ceremonies. URL: https://zkproof.org/2021/06/30/setup-ceremonies/
19. Zcash Foundation. Conclusion of the Powers of Tau Ceremony, 2018. URL: https://zfnd.org/conclusion-of-the-powers-of-tau-ceremony-2/
20. Zcash. Parameter Generation. URL: https://z.cash/technology/paramgen/
21. Zooko Wilcox, Ian Sagstetter, 2022, November. Electronic Coin Co. Halo's contribution goes beyond efficiency. URL: https://electriccoin.co/blog/halos-contribution-goes-beyond-efficiency/
22. Electronic Coin Company, 2019, September. Halo: Recursive Proof Composition without a Trusted Setup. URL: https://electriccoin.co/blog/halo-recursive-proof-composition-without-a-trusted-setup/
23. Bowe, S., Grigg, J. and Hopwood, D., 2019. Recursive proof composition without a trusted setup. Cryptology ePrint Archive.
24. The halo2 Book. URL: https://zcash.github.io/halo2/
25. Miller, A., Möser, M., Lee, K. and Narayanan, A., 2017. An empirical analysis of linkability in the monero blockchain.(2017). arXiv preprint arXiv:1704.04299.
26. Möser, M., Soska, K., Heilman, E., Lee, K., Heffan, H., Srivastava, S., Hogan, K., Hennessey, J., Miller, A., Narayanan, A. and Christin, N., 2017. An empirical analysis of traceability in the monero blockchain. arXiv preprint arXiv:1704.04299.
27. Justin Ehrenhofer (SamsungGalaxyPlayer) and the Monero community, 2017, April. An Unofficial Response to "An Empirical Analysis of Linkability in the Monero Blockchain". URL: https://www.getmonero.org/2017/04/19/an-unofficial-response-to-an-empirical-analysis-of-linkability.html
28. Justin Ehrenhofer (SamsungGalaxyPlayer), 2018, March. Response to "An Empirical Analysis of Traceability in the Monero Blockchain", Version 2 URL: https://www.getmonero.org/2018/03/29/response-to-an-empirical-analysis-of-traceability.html
29. Jonathan "Duke" Leto, 2019. Zcash Metadata Leakage CVE-2019-16930. URL: https://duke.leto.net/2019/10/01/zcash-metadata-leakage-cve-2019-16930.html
30. Anonymity Networks with Monero. URL: https://github.com/monero-project/monero/blob/master/docs/ANONYMITY_NETWORKS.md
31. Diego Salazar, 2020. How Dandelion++ Keeps Monero's Transaction Origins Private. URL: https://localmonero.co/knowledge/monero-dandelion?language=en
32. Tramèr, F., Boneh, D. and Paterson, K., 2020. Remote Side-Channel Attacks on Anonymous Transactions. In 29th USENIX security symposium (USENIX security 20) (pp. 2739-2756).

33. Mercer, R., 2016. Privacy on the blockchain: Unique ring signatures. arXiv preprint arXiv:1612.01188.
34. Garethtdavies, 2019, September. Measuring Shielded Adoption. URL: https://forum.zcashcommunity.com/t/measuring-shielded-adoption/35022
35. CryptoNight. URL: https://monerodocs.org/proof-of-work/cryptonight/
36. Moneropedia. Ring Size. URL: https://www.getmonero.org/resources/moneropedia/ring-size.html
37. LNCS Homepage, http://www.springer.com/lncs. Last accessed 4 Oct 2017
38. Ben-Sasson, E., Chiesa, A., Tromer, E. and Virza, M., 2014. Succinct Non-Interactive zero knowledge for a von neumann architecture. In 23rd USENIX Security Symposium (USENIX Security 14) (pp. 781-796).
39. Fungibility, Moneropedia. URL: https://www.getmonero.org/resources/moneropedia/fungibility.html
40. Kappos, G., Yousaf, H., Maller, M. and Meiklejohn, S., 2018. An empirical analysis of anonymity in zcash. In 27th USENIX Security Symposium (USENIX Security 18) (pp. 463-477).