A Comparison of Monero and Zcash

Håvard Anda Estensen
haavard.ae@gmail.com

June 13, 2018

Abstract

There is a lot of excitement (and hype) around blockchain. Since most of the blockchains rely on a public ledger, transactions are pseudonymous and fully traceable. This paper will examine and compare how two popular cryptocurrencies, Monero and Zcash achieve privacy by obfuscating transactions.

1 Introduction

Cryptocurrencies like Bitcoin (BTC) is revolutionizing the way digital payments are done. The systems are designed to work without an intermediary, directly between users. This is done by recording transactions on a public distributed ledger - a blockchain. Users that provide CPU power to the network are called miners and are rewarded with the network currency.

But transactions are not as private as a lot of people think. Web merchants routinely leak data about purchases[1] and once one purchase is compromised the all purchases linked to an account is compromised since all transactions are recorded on the blockchain.

In this paper, BTC will be used as a baseline comparison against Monero and Zcash. This makes a good comparison as both Monero and Zcash are hard forks of Bitcoin.

2 Why Privacy Is Important

To understand why BTC doesn't provide desired privacy properties it is necessary to take a step back to look at how the core technology works.

2.1 Blockchain

A blockchain is an append-only list of blocks that are linked and secured with cryptography[2]. Each block contains transaction data, a timestamp and the cryptographic hash of the previous block. A blockchain is protected against modification of blocks by employing a data structure called a Merkle tree. In a Merkle tree, each parent node contains a hash of the child node so it is only necessary to compare root nodes of two files to see if they are the same.

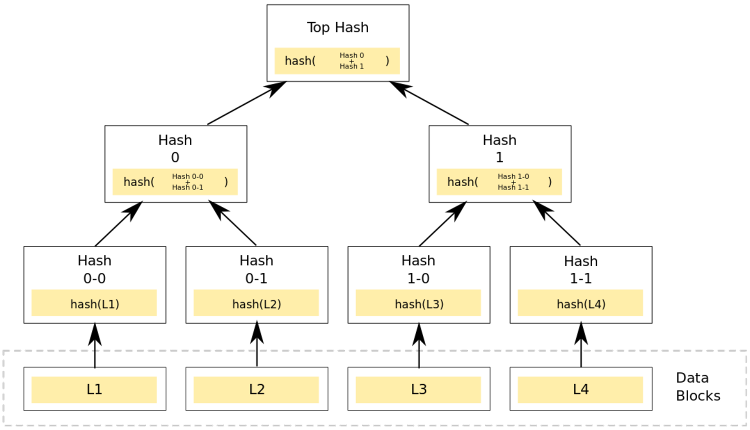

Figure 1: Merkle Tree

For each block added to the blockchain, it becomes harder to change a previous block. This is because one needs the majority of the hashing power in the network to do so. And like amber, the more layers that are added the harder it becomes to undo. But most systems are still based on probability and actual permanence is not guaranteed.

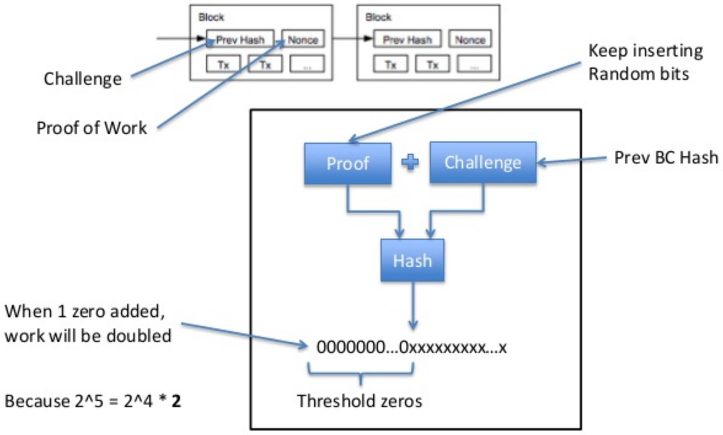

Figure 2: Proof-of-work

Most blockchains use a proof-of-work (PoW) algorithm to add blocks to their blockchain. Miners brute force a cryptographic hashing algorithm to find a solution that starts with a given number of zeros. As more hashing power is added to the network this value is automatically adjusted by the network to make it harder to find a solution. A nice property of cryptographic hashing functions is that it is very fast to verify a solution. And since each block is dependent on the previous one, it is not possible to pre-compute a solution and everyone starts over once a block is added. Figure 2 illustrates how this work for Bitcoin.

2.2 How Bitcoin Works

To be able to receive BTC you generate a public address and share that with the person you want to send you funds. A public address might look like this:

$1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX$

When someone sends you funds they announce to the whole network that these funds now belong to you. This is called a transaction.

Transactions are collected into blocks that are processed by miners. Before accepting a transaction, the miners verifies that the transaction is valid and that double-spending did not occur.

Approved transactions are irreversible when buried under enough confirmations, so if funds are sent to the wrong public address they are stuck until someone with the corresponding private key can unlock them.

2.3 Why You Should Care About Privacy

If you go and buy coffee you would be revealing your salary to the coffee shop owner and what you do in your spare time with your employer. You would leave a public breadcrumb trace of where you have been. You might say that ”I have nothing to hide”, but what if you didn’t know you were doing something wrong in the first place? Wired magazine wrote[3] an article about it and claims you can go to jail for being in possession of a lobster under a certain size. No matter if you bought it in a store, found it after it died of natural causes or even killed it while acting in self-defense. Law is complex and it might be unreasonable to require everyone to be aware of all of it. If law enforcement was 100% effective you would not be able to progress. How could it be decided that marijuana should be legal if no one had used it?

”But I don’t receive my salary in BTC”. But it was still acquired in some way. At some point, the BTC you have was bought for fiat and that can be traced. Even if you bought it with cash from a friend police or criminals can go back and threaten your friend. If you got the BTC by mining the IP addresses can be traced to you. There are a lot of tracks to cover!

2.4 Privacy Properties

We don’t want anyone to know when we spend money. Unlinkability is when you can’t tell who sent money. If someone sends money twice you can’t even tell that it is the same person sending money.

Another desired property is to not be able to trace funds. If someone knows you have money they should not be able to tell when you spend it. This is called untracability. This also makes the money fungible.

Units can’t be blacklisted If a coin has been used in an illegal transaction in the past the history will be contained in the blockchain and certain businesses can be obliged to not accept BTC that has been touched by certain entities. These entities do not necessarily conduct illegal activities, but maybe only unsavory activities. Yes, this will also make it possible for criminals to hide their activity. But so is allowing encrypted communications.

Further discussion about the political side of private cryptocurrencies goes outside the scope of this paper.

3 Zcash

On blockchains everything is public. By encrypting transactions we face another problem: How can we verify that transactions are valid? Zcash use zero-knowledge proofs! Transactions in Zcash where the source, destination and amount are obscured are called shielded transaction. But this is optional and can lead to linkability[4].

Zcash tries to balance privacy and transparency be enabling selective disclosure[5]. Transactions are auditable but under the participants' control.

3.1 Zero-Knowledge Proofs

A zero-knowledge (zk) proof can prove a statement about a secret without giving up that secret. Even though the theory behind it was discussed in the 1985 paper "The Knowledge Complexity of Interactive Proof Systems"[6], which the authors got the Turing award for[7], it has not gone mainstream before now. This can seem counterintuitive at first, and the math is rather hard. But with an example, one can convince even people without a background in cryptography that zero-knowledge proofs are possible at all.

Imagine that you have two pens, one red and one blue, and want to prove to a colorblind person that you indeed have different-colored pens. Give the pens to the other person and make them hold one in each hand. Then let them put them behind their back and shuffle them. Or not. When they show them to you again you can tell them if the shuffle was done or not. Of course, you could have guessed and would have had a 50% probability of guessing right. But by doing this multiple times the probability that you guess diminishes. After n correct identifications the probability that you guessed is 0.5^n and we can establish confidence that you can identify one pen from the other.

There are three key properties for a zero-knowledge protocol. Correctness: Both parties must be honest. Soundness: If you don't know the secret you can't prove it. Zero-knowledge: If the protocol is followed nothing new is learned. For our pen example notice that no information about which pen is red or blue is leaked. Only that they are distinguishable.

In the real world, the pens are replaced by a digital commitment scheme. This allows one party to commit a given message but keeping it secret by encrypting it and later giving everyone the key to decrypt the message.

However, zk's face another problem: it is still a 2 round protocol in which the two parties have to communicate. We would like no communication between the prover and the verifier. This is where zk-SNARKS enter.

3.2 zk-SNARKS

zk-SNARKS is a new form of zero-knowledge cryptography and Zcash is the first widespread usage of it[8]. It is an acronym for Zero-Knowledge Succinct Non-Interactive Argument of Knowledge and allows non-interactive zero-knowledge proofs.

In the earlier described zk protocol the two parties had to communicate back and forth for multiple rounds, but with SNARKS the proof consists of only a single message sent from prover to verifier. To produce this proof there is a setup phase where a reference string is shared. In Zcash this is a multi-party computation and is the parameters for the zk-SNARK. If the randomness used to generate these parameters is compromised by an attacker they can be used to construct false proofs. The secret randomness each participant has is referred to as "toxic waste" and is destroyed to protect the integrity of the protocol. Only one participant needs to be honest for the protocol to work and the more participants the lower the chance of collusion. Until now the multi-party protocol (Sprout) has not scaled to more than a handful of users.

3.3 Red Flags

The reliance on a trusted setup might be the biggest weakness in Zcash[9]. While there is no evidence that the multi-party computation (Power of Tau Ceremony) was compromised one still have to trust that the participants won't collude and secretly print Zcash for themselves. The next major update[10] (Sapling) scheduled for release in late June 2018 will address this and drastically increase the performance with a new elliptic curve called JubJub.

Zcash is a privately owned company based in the United States and can, therefore, receive a subpoena by regulators.

4 Monero

While zk-SNARKS makes up the core of Zcash's obfuscation Monero uses multiple different techniques to make transactions private. Compared to Zcash transactions are also private by default.

4.1 Stealth Addresses

Stealth addresses protect a receiver of a transaction by making the sender creating a new address for every transaction[11]. All Monero accounts have two keys: a view key and a spend key. The view key is used when scanning the blockchain to see if there are any transactions destined for you. This is why when launching a Monero wallet it will scan the blockchain.

4.2 Ring Signatures

To obfuscate the sender Monero relies on ring signatures. A ring signature is a digital signature that can be performed by any member of a group of user that each has keys[12]. A message signed with a ring signature proves that the message is signed by someone in a group, but makes it computationally infeasible to compute who signed it. Ring signatures enable transaction mixing by mixing the funds that are sent with other users funds. The exact coin you sent might end up being sent to another user than you wanted to send it to. But because of fungibility, it does not matter. Two coins are worth the same.

4.3 Ring Confidential Transactions

Ring confidential transactions (RingCT) is an improved version of ring signatures which also hides the amount that is sent[13]. This prevents blockchain analysis attacks that based on the amount that was sent.

The internet traffic to Monero nodes is not hidden, so anyone monitoring your internet can see that you are using Monero and think that you have something to hide. This is scheduled to be fixed by implementing Invisible Internet Project (I2P). The project, called Kovri, protects users at the protocol level.

4.4 Red Flags

The promised unlinkability has not worked as promised. For transactions done between 2014 and 2016 about 62% of them can be linked. [14]

5 Conclusion

Privacy is an ongoing arms race between researchers and attackers. Software cannot be guaranteed bug-free or guarantee privacy. Using privacy-centric cryptocurrencies to break laws are probably not a good idea. Having all nodes verify all transactions are expensive and adding privacy properties provides even more overhead. Trusting users to follow security best-practices might be expecting too much before they comprehend what public key cryptography is. Privacy should, therefore, be as non-invasive as possible to reduce friction so users can focus on spending and not the cryptocurrency itself.

References

[1] S. Goldfeder, H. A. Kalodner, D. Reisman, and A. Narayanan, “When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies,” *CoRR*, vol. abs/1708.04748, 2017.

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

[3] "Why I Have Nothing To Hide Is the Wrong Way to Think About Surveillance." https://www.wired.com/2013/06/why-i-have-nothing-to-hide-is-the-wrong-way-to-think-about-surveillance/. [Online; accessed June-10-2018].

[4] J. Quesnelle, "On the linkability of zcash transactions," *CoRR*, vol. abs/1712.01210, 2017.

[5] "How Zcash Tries to Balance Privacy, Transparency in Blockchain." https://www.americanbanker.com/news/how-zcash-tries-to-balance-privacy-transparency-in-blockchain. [Online; accessed June-13-2018].

[6] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems," *SIAM J. Comput.*, vol. 18, pp. 186–208, Feb. 1989.

[7] "Goldwasser and Micali win Turing Award." http://news.mit.edu/2013/goldwasser-and-micali-win-turing-award-0313. [Online; accessed June-8-2018].

[8] "What are zk-SNARKs?." https://z.cash/technology/zksnarks.html. [Online; accessed June-8-2018].

[9] "Announcing the world's largest multi-party computation ceremony." https://z.cash.foundation/blog/powers-of-tau/. [Online; accessed June-8-2018].

[10] "Cultivating Sapling: Faster zk-SNARKs." https://blog.z.cash/cultivating-sapling-faster-zksnarks/. [Online; accessed June-8-2018].

[11] "Stealth Address." https://getmonero.org/resources/moneropedia/stealthaddress.html. [Online; accessed June-10-2018].

[12] "Ring Signature." https://getmonero.org/resources/moneropedia/ringsignatures.html. [Online; accessed June-10-2018].

[13] S. Noether, A. Mackenzie, and the Monero Research Lab, "Ring confidential transactions," *Ledger*, vol. 1, no. 0, pp. 1–18, 2016.

[14] "Revealing the hidden links in the Monero blockchain." http://hackingdistributed.com/2017/04/19/monero-linkability/. [Online; accessed June-10-2018].