Privacy-centric cryptocurrencies

W.J.B. Beukema

May 2015

1 Background

1.1 Bitcoin

Bitcoin [7] is at this moment the most popular e-cash currency. The design of the Bitcoin as a currency is fundamentally different from traditional currencies. Whereas traditional currencies depend on central authorities, the Bitcoin system relies on a decentralised network of volunteers in order to transfer money. As there is no single point of trust, the validity of transactions is guaranteed when more than 50% of the participants is honest. Because this is achieved by using mathematical models and cryptographic proof, the entire Bitcoin system is based on mathematical proof instead of trust [7].

1.2 Anonymity

Although Bitcoin is based on principles such as transparency and flexibility, privacy was not a primary design goal of Bitcoin. Bitcoin provides some degree of privacy through *pseudonimity*, as one user can virtually make as many Bitcoin addresses as he wishes to send bitcoins[1] to and from. However, in order to provide transparency, Bitcoin is designed in such a way that every single transaction is visible to anyone through the blockchain (the public ledger). This includes the sender's address, the recipient's address, the amount of bitcoins transferred, but also the history of the money flow (i.e., how the sender obtained the bitcoins he is transferring in the transaction). Therefore, the pseudonimity does not provide full privacy, as it is still possible to analyse the flow of bitcoins, which might link certain Bitcoin addresses or even reveal the identity of the owner of the Bitcoin addresses.

[1] We distinguish to different contexts in which the term 'Bitcoin' may be used:

- *Bitcoin* refers to the system as described by Nakamoto [7];
- *bitcoin(s)* or *BTC* refers to the currency unit (like euro and €, respectively);

In order to provide a greater level of anonymity, a number of commercial parties provide a so-called *mixing service*[2], also known as *laundries* or *tumblers*. A user can send his bitcoins to this party, which will try to confuse the money trail. Usually, this is done by adding the bitcoins into a large pool and then, after some interval, the user will be able to retrieve the same number of bitcoins from the pool, but different coins.

Unfortunately, there are some serious risks attached to the use of such services. A user has to fully trust the operator, as the operator might steal the funds it has received. Also, as has happened some times, Bitcoin services go out of business suddenly, taking the funds with them. Another issue is that there is no complete anonymity, as the operator can still trace back the money. The operator might abuse the information or this information might be stolen, as the user usually has no guarantees over the security of the operator itself. Finally, the interval before reclaiming the bitcoins should be large enough to allow enough coins to be mixed in.

2 Literature

2.1 Zerocoin

To implement the concept of a mixing level on protocol level, Miers et al. [6] proposes an extension of Bitcoin, called *Zerocoin*. In this proposal, bitcoins can be temporarily converted to zerocoins, which are all stored in an escrow pool in the blockchain.

In order to *mint* a zerocoin (i.e., convert a bitcoin to a zerocoin), one has to generate a random serial number S and random number r and encrypt this into a coin C using a commit scheme. The coin C is added to a (strong RSA one-way) accumulator by miners and the amount of bitcoins is added to the zerocoin escrow pool. To obtain the original bitcoins, the owner has to prove (using a zero-knowledge proof) that it knows a coin C in the escrow pool (without revealing which C), and that it knows a number r that along with the serial number corresponds to a zerocoin (without revealing the value of r). This proof, along with serial number S, is included in a zerocoin spend transaction. Miners have to verify that the proof is correct and that serial number S has not been claimed before (preserving Bitcoin's double spending resistance). Note that each zerocoin corresponds to one bitcoin (or a predefined number of bitcoins), which means that transactions whose values are lager than 1 BTC result in multiple Zerocoin transactions.

The advantage of the approach Zerocoin has, is that it gives stronger anonymity guarantees than mixing services, as this scheme is implemented on protocol level and relies on mathematics. If the security parameters are set in the right way, the authors claim de-anonymising a single zerocoin is

[2]Examples include Anonimcoin, BitLaundry, Bitcomix and BitcoinFog.

infeasible.

However, the proofs necessary to claim zerocoins introduces a significant overhead for participants in the network. Compared to the traditional Bitcoin protocol, additional time is necessary to verify the proof and the size of a transaction would increase drastically, creating more network traffic. Also, Zerocoin does not hide the amount of the transaction, which might still reveal sensitive information and might lead to the link between an individual and an address.

2.2 Zerocoin improvements

Shortly after Zerocoin was presented, there have been several suggestions to improve its design. Androulaki and Karame [1] suggest an extension of Zerocoin called *EZC* in which transaction amounts and account balances are hidden. In this system, it is also possible to use minted coins in a transaction, thus without converting them back to bitcoins, as is required in Zerocoin. These transactions will only reveal the transaction amount to the sender and receiver.

Another variant, the *Pinocchio Coin* [4], tries to increase the performance of Zerocoin by replacing the Strong RSA based accumulator by a solution that relies on elliptic curves and bilinear pairings. The authors claim that this results in smaller proofs and quicker verification.

A year after the initial Zerocoin paper was published, the same authors presented an improved design [5]. An important difference with the original design is that the overhead is lowered by reducing the level of security in such a way that it is still safe enough. While the original paper assumed that all proofs must be computationally infeasible to forge, the new publication takes a more practical approach: it should be harder to forge a single zerocoin than the (Bitcoin) block mining process. Together with some other enhancements, the authors claim that the proof size can be reduced from 25KB to 10KB and the proving time from 0.5 seconds to 0.25 seconds. Although as a result the security level is lower, it is claimed that it is still economically irrational to perform an attack.

2.3 Zerocash

Despite the suggested improvements, Zerocoin still lacked some properties that are necessary to make the currency a serious alternative to existing cryptocurrencies. Some of the authors of the Zerocoin paper, together with some others, contributed to another cryptocurrency that can be seen as the successor of Zerocoin, called *Zerocash*[2]. It is based on the same principles as Zerocoin, but uses different methods to make it significantly more efficient than its predecessor. Unlike Zerocoin, which was intended as an extension

for Bitcoin, Zerocash is suggested to be a fork of Bitcoin (making it a so-called *altcoin*).

The authors claim to have reduced the proof size to less than 1KB and under 6ms to verify. To achieve this, Zerocash now uses a hash function (SHA-256) for commitments, it uses Merkle Trees instead of accumulators and a zero-knowledge Succinct Non-interactive Arguments of Knowledge (*zk-SNARKs*), as suggested by Danezis et al. [4]. Also, the new protocol also allows, similar to the approach of Androulaki and Karame [1], to make direct payments in Zerocash that hides both the origin and the amount of the payment. Finally, Zerocash is a divisible currency, making payments more flexible than in Zerocoin.

2.4 Privacy-centric cryptocurrencies and criminality

Although there are many reasons why it is reasonable to expect some level of privacy from a cryptocurrency, it might also open the door to criminal activity, it has been argued. If amounts, balances and sender/recipients are hidden, combined with the absence of a central authority, cryptocurrencies can be abused for criminal purposes such as money laundering. This might also hinder the acceptance of cryptocurrencies as a replacement for traditional currencies.

There has been research into how cryptocurrencies can somehow prevent this abuse from happening. A way to make it harder to launder money has been suggested by Camenisch et al. [3]. The authors suggest building in policies in e-currencies that once the total transaction amount exceeds some threshold, the payments are not private anymore. Zerocash claims to be able to enforce such policies on protocol level [2].

References

[1] E. Androulaki and G. Karame. Hiding transaction amounts and balances in bitcoin. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8564 LNCS:161–178, 2014. doi: 10.1007/978-3-319-08593-7_11.

[2] E. Ben-Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza. Zerocash: Decentralized anonymous payments from bitcoin. pages 459–474, 2014. doi: 10.1109/SP.2014.36.

[3] J. Camenisch, S. Hohenberger, and A. Lysyanskaya. Balancing accountability and privacy using e-cash. In *Security and Cryptography for Networks*, pages 141–155. Springer, 2006.

[4] G. Danezis, C. Fournet, M. Kohlweiss, and B. Parno. Pinocchio coin:

Building zerocoin from a succinct pairing-based proof system. pages 27–29, 2013. doi: 10.1145/2517872.2517878.

[5] C. Garman, M. Green, I. Miers, and A. Rubin. Rational zero: Economic security for zerocoin with everlasting anonymity. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8438:140–155, 2014. doi: 10.1007/978-3-662-44774-1_10.

[6] I. Miers, C. Garman, M. Green, and A. Rubin. Zerocoin: Anonymous distributed e-cash from Bitcoin. pages 397–411, 2013. doi: 10.1109/SP.2013.34.

[7] S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. May 2009. URL `http://www.bitcoin.org/bitcoin.pdf`.