CRYPTIX LABS

Privacy Taxonomy
Part One: Privacy Coins

Whilst there are numerous cryptocurrency privacy projects, many of these are aimed towards patching privacy issues in existing blockchains or instead creating private infrastructure.

This document will focus on cryptocurrencies that have privacy-preservation 'baked in': two of the longest-standing blockchains, Monero and Zcash, relative-newcomers Grin and Beam, and still-in-testnet Mobilecoin. Each cryptocurrency is unique and utilizes different methods to maintain privacy, and as such this overview document also serves a secondary purpose as a crash-course in different technical approaches to privacy-preservation in cryptocurrencies.

First to be discussed is Monero. The Monero protocol - Cryptonote - was created by an author (or group of authors) under the pseudonym of Nicolas Van Saberhagen. It implements *stealth addresses, ring signatures,* and *ring confidential transactions*, anonymising a transaction's receiver, sender, and amount respectively. *Stealth addresses* avoid the issue of 'linkage' between two parties via transactions in that, when sending a transaction to account, this transaction is actually sent to a one-time address created specifically for this purpose. This one-time address is not linked publicly to the receiver's address. As such, even if Alice repeatedly sends transactions of which Bob is the recipient, none of transactions should in theory be able to be linked, or even understood as multiple transactions with the same recipient, as Bob's address is not appearing on the blockchain. *Ring signatures* anonymise the sender of a transaction; as every transaction must be signed with a key, in the example above it would seem that whilst Bob remained anonymous, Alice's address - being the sender of multiple transactions - would be made public on the blockchain as it was with her key that the transaction was signed. However, Monero groups multiple keys into a 'ring' with every transaction, of which there is an equal possibility that any of these keys is the one that signed the transaction. As such, analysis of transactions becomes unfeasibly complex. Whilst this does not exactly anonymise Alice - in that her key is part of the ring involved in signing the transaction - it does satisfactorily obfuscate its being used for a specific transaction. *Ring confidential transactions (RingCT)* are the final piece of this tripartite technique by "applying a mathematical function to all funds such that public observerscan see that the transactions are legitimate, but only the sender and receiver can know the actual amounts."[1] In other words, all public observers of the Monero blockchain can see is that one of a ring of signatures was used to sign a transaction, that this transaction was valid, and that this transaction was received by a one-time address that is not linked to any other address, making analysis of transactions in order to deanonymize participants in the blockchain incredibly difficult if not impossible.

Zcash offers much the same as Monero with regards to anonymising a transaction's amount, sender, and receiver. It relies on *Zero-Knowledge Succinct Non-interactive pRoofs of Knowledge* (zk-SNARKS) in order to achieve this, an instance of zero-knowledge proof systems[2] which themselves stem from academic computer science and complexity theory. Whilst this would seem to grant Zcash an advantage over Monero off the bat, there is one major disadvantage to using zk-SNARKS - their need for a 'trusted setup'. This setup involves setting the parameters for transaction construction and verification in the network, the information - referred to as 'toxic waste' - used in which must remain secret, in order to prevent malicious actors from creating proofs for Zcash that appear valid but are in fact not. Whilst there have been attempts to assuage fears that this information was in fact not destroyed[3], the fact that this is not able to be computationally verified does stand as an issue for many privacy advocates in the blockchain space.

Grin and Beam, although newer than Zcash and Monero, offer an opportunity for an interesting comparison.[4] They are both implementations of the same consensus mechanism: Mimblewimble. As with many early cryptocurrency publications, Mimblewimble was introduced by an author (or authors) under the name of 'Tom Elvis Jedusor',[5] and was originally intended to patch issues that had cropped up regarding both scaling and privacy in Bitcoin. It employs a model in which *confidential transactions* are used, wherein *blinding factors* are used to encrypt the amount sent in a transaction for everyone aside from the sender and receiver. This is a random value chosen by the sender, and is used as *proof of ownership* when the receiver is then wanting to themselves create a transaction. The validity of a transaction is assessed simply by comparing the number of transaction inputs and outputs, thus stopping the creation of invalid transactions whilst retaining privacy. Neither Grin nor Beam implement a model which uses addresses, visible transaction amounts, or transaction history: the Mimblewimble protocol is a very stripped down protocol offering private and secure transactions coupled with very small block sizes, and lacks the need for the trusted setup of zk-SNARKS and the computationally-intensive procedures of Monero. Whilst there was a supposed vulnerability found in Mimblewimble several years ago,[6] the scope of the issue was overstated and seemed to be based on a misunderstanding of the information that could be garnered from the vulnerability.[7] The one issue that Mimblewimble does have is one shared by many privacy-oriented technologies: "[y]ou never achieve greater privacy than the size of your anonymity set".[8] This, however, is simply a fact of life for these technologies, and as such cannot be considered an issue that is due to poor technical development.

Finally, and still in testnet phase, is Mobilecoin. As suggested by its name, Mobilecoin takes a different approach to the above privacy coins with their hardwallet- or CLI-oriented development by focussing on seamless mobile app integration. Relying on the Stellar Consensus Protocol,[9] and a server-based node model wherein all transactions and accounts are hidden by default, time will tell as to whether this model works, but this architecture is sure to raise a few concerns amongst privacy-advocates in the cryptocurrency space.

All of these different solutions have numerous pros and cons. Privacy-preserving technology is an arms race that is constantly in flux; each new development brings about new academic research finding potential flaws in these developments.

[1] https://www.monero.how/how-does-monero-work-details-in-plain-english
[2] A primer to which can be found here: https://blog.cryptographyengineering.com/2014/11/27/zero-knowledge-proofs-illustrated-primer/
[3] See information on Multi-Party Computation Ceremonies: https://z.cash/technology/paramgen/
[4] On a more meta-level these coins could be good for a case study regarding the difference in reception etc between community-funded and VC-funded coins, but this will be saved for a separate document.
[5] https://www.coindesk.com/cryptographer-voldemort-bitcoin-scaling
[6] https://medium.com/dragonfly-research/breaking-mimblewimble-privacy-model-84bcd67bfe52
[7] https://medium.com/grin-mimblewimble/factual-inaccuracies-of-breaking-mimblewimbles-privacy-model-8063371839b9
[8] Ibid.
[9] https://www.stellar.org/papers/stellar-consensus-protocol is an arms race that is constantly in flux; each new development brings about new academic research finding potential flaws in these developments.