Academic Papers

Zerocoin: Anonymous Distributed E-Cash from Bitcoin (Ian Miers, Christina Garman, Matthew Green, Aviel D. Rubin)

This is the original Zerocoin paper that forms the foundation of our privacy protocol. Zcoin was the first to implement this protocol in September 2016.

Improvements to libzerocoin that solved two flaws was identified by Tim Ruffing when engaged to audit Zerocoin by Zcoin. These improvements have been incorporated and are now live.

MTP: Egalitarian Computing (Alex Biryukov, Dmitry Khovratovich) (revision and improvement funded by Zcoin)

MTP is the Proof of Work algorithm that Zcoin uses that promotes egalitarian mining while maintaining quick verification. The original paper had flaws as identified by Dinur and Nadler. Zcoin organized a bounty to harden MTP and also funded research to solve these issues as reflected in the linked paper. MTP was coded from the ground up by Zcoin and switched to the MTP algorithm in December 2018.

Dandelion++ Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees (Giula Fanti et al)

Dandelion++ was originally developed for Bitcoin as a way to obscure the origin of transactions by changing the way transactions propagate through the network. Dandelion++ is slated to go live on Bitcoin Core 0.18. Zcoin was the first project to go live with Dandelion++ on mainnet in September 2018.

One-out-of-Many Proofs: Or How to Leak a Secret and Spend a Coin (Jens Groth et al)

One out of Many Proofs forms the foundation of Sigma which improves on Zerocoin by removing trusted setup and reducing proof sizes. Zcoin is also applying some further efficiency modifications to the original paper. Sigma is in development and is slated to be released in Q1 2019.

Lelantus: Private transactions with hidden origins and amounts based on DDH (Aram Jivanyan)

Lelantus is Zcoin's next generation privacy protocol which improves on Sigma by removing the requirement of fixed denominations allowing people to mint arbitrary amounts and spend partial amounts without revealing values. The Lelantus paper is still under development and is seeking peer review. Coding on the cryptographic libraries of Lelantus has begun. Lelantus is Zcoin's own innovation.