An Empirical Analysis of Anonymity in Zcash, by George Kappos

Introduction: Zcash is the cryptocurrency platform with the strongest anonymity guarantees. It has market capitalization of over 1 billion USD during paper was written and it uses shielded pool to improve security. The paper investigate all the facts of anonymity in Zcash's transactions,ranging from its transparent transactions to the interactions with and within its main privacy feature, a shielded pool that acts as the anonymity set for users wishing to spend coins privately. The paper provide the first in-depth empirical analysis of anonymity in Zcash,in order to examine these claims and more generally provide a longitudinal study of how Zcash has evolved and who its main participants are.

Zcash transactions: Zcash allows four types of transactions which includes Transparent transactions, Shielded transactions, Private transactions, Deshielded transactions. Any transaction which interacts with the so-called shielded pool in Zcash does so through the inclusion of a vJoinSplit The input includes list of input t-addresses, two double spending tokens, zero knowlegde proof and the output includes list of output t addresses, two shielded outputs and an encrypted memo field.

Zcash Participants: There are four types of participants who interacts with Zcash network. Founders took part in the initial creation and release of Zcash, and will receive 20 % of all newly generated coins. Miners take part in the maintenance of the ledger, and in doing so receive newly generated coins. Services are entities that accept ZEC as some form of payment. . Users are participants who hold and transact in ZEC at a more individual level.

Zcash Blockchain Statistics: The research last parsed the block chain on January 21 2018, at which point 258,472 blocks had been mined. Overall, 3,106,643 ZEC had been generated since the genesis block, out of which 2,485,461 ZEC went to the miners and the rest (621,182 ZEC) went to the founders.

Heuristics for T-address clustering: Heuristic 1. If two or more t-addresses are inputs in the same transaction (whether that transaction is transparent, shielded,or mixed),then they are controlled by the same entity. Heuristic 2. If one (or more) address is an input t address in a vJoinSplit transaction and a second address is an output t-address in the same vJoinSplit transaction, then if the size of zOut is 1 (i.e., this is the only transparent output address),the second address belongs to the same user who controls the input addresses.

Tagging Addresses The research identified the top ten Zcash exchanges. It also collected the publicized addresses of the founders, as well as addresses from known mining pools. If the recipient of the coingen transaction in a given block was tagged as belonging to a given mining pool then it checked to see that the block had been advertised on the website of that mining pool.

Conclusions: The research applied both well-known clustering heuristics that have been developed for Bitcoin and attribution heuristics developed that take into account Zcash's shielded pool and its unique cast of characters.The participants who do engage with the shielded pool do so in a way that is identifiable, which has the effect of significantly eroding the anonymity of other users by shrinking the overall anonymity set.

Future Works it may be possible to classify more z-to-z transactions by analyzing the time intervals between the transactions in more detail, or by examining other metadata such as the miner's fee or even the size (in bytes) of the transaction. The interesting regulatory question whether or not mainstream exchanges would continue to transact with Zcash if it switched to supporting only z-addresses