Empirical analysis of the Zcash blockchain

CryptoLUX Research Group

University of Luxembourg

1 Introduction

Our proposal is the empirical analysis of the Zcash blockchain. Despite Zcash positioning itself as a privacy-preserving blockchain, still about 80% of all the transactions are transparent, which makes them suitable for analysis. Until the Sapling update is released, and private transactions are made mandatory, there can be unintended vulnerabilities concerning the privacy of the users, and those problems may surface with an empirical analysis.

2 Technical Approach

Our goals would be to investigate existing approaches for Bitcoin analysis, and apply and extend them to the Zcash blockchain as the structure of the public transactions are the same as in Bitcoin. On the other hand as Zcash is focused on privacy, the privacy implications of these approaches, especially for the case of transactions between a deanonymized user and a z-address could lead to unforeseen consequences.

In the following sections we will list our planned tasks, describe them in more detail and estimate how much work would they require.

2.1 Extending or Creating a Tool

Using existing or our own tools. We are currently investigating the Blocksci tool by the researchers at Princeton University, but we found that it does not support Zcash as a blockchain natively, because the nonces of Bitcoin blocks are integers, while in Zcash they are 256 bit hex strings. That means that the publicly available code of Blocksci is not working on the Zcash database, and there are further differences as well that prevent a direct adaption of the tool. We could overcome some of these problems but not all yet. If we decide to use an existing tool we need to modify and publicly fork from an existing codebase in order to have full support of Zcash. This means extending these tools with new functionalities specialized for Zcash transactions. If we decide otherwise, we will write our own tool specifically designed for Zcash analysis, and we would make that available to the public as well.

This task would be done in an estimate 1.5 person months of work to develop the basic functionalities. Afterwards each task would create a new module for the tool.

2.2 JoinSplit Transactions with Public Known Addresses

Analyzing big clusters of addresses, like marketplaces, exchanges, where our focus would be on transactions between z- and t-addresses, as for transactions between t-addresses the existing Bitcoin approaches would mostly work without any significant tweaks. The task would last about 2 person months of work.

2.3 Patterns of Usage

Investigating general JoinSplit transactions between t- and z-addresses, whether there are patterns of misuse that would lead to the deanonymization of a z-address holder. A detectable pattern would be for example somebody moving currency first to a z-address, and then in a short time frame there is a transaction from a z-address to a t-address with similar amount of currency. The task would take an estimated 2 person months of work.

2.4 Network Analysis

Analyzing the network properties of the blockchain as well, as our team has expertise in the topic [BKP14]. The task would take an estimated 1.5 person months of work.

2.5 Prediction of Transaction Fees

Empirical analysis of transactions to provide a more accurate prediction of the transaction fees for wallet implementations, as currently users are usually either overpaying, or waiting too long for their transactions to be accepted, while with a more accurate estimate these problems could be mitigated. The task would take and estimated 1 person month of work.

2.6 Privacy Implications of SPV Wallets

Investigation of the privacy implications of SPV wallets in Zcash, as Bloom filter based light wallets in Bitcoin can lead to privacy related attacks [GCKG14]. Our plan is to spend around 1 person month of work on the task.

3 Team

The team that would work on the project would consists of PI Alex Biryukov, and two of his PhD students, Daniel Feher and Sergei Thikomirov. We might use expertise from other members of CryptoLUX team if necessary.

4 Security Considerations

The work will be done in ethical way, no individual data would be deanonymized, results of experiments on real data would not be stored. For demonstration purposes we will deanonymize our own transactions. We have prior experience with our studies of privacy in Tor and Bitcoin on how to carry such work in an ethical way.

5 Schedule

We have already started working on this project, and will probably continue even if we are not selected for funding in this round (however in such case our person-month effort would probably be reduced to one person working on this project). The project would take 9 person months of work, which are divided in the following way and order:

- Task 1 - Extend or create the Zcash blockchain scanning tool (1.5 person months) (Section 2.1)
- Task 2 - JoinSplit transactions with public known large clusters of addresses (2 person month) (Section 2.2)
- Task 3 - Look for patterns of usage between z- and t-addresses in general (2 person months) (Section 2.3)
- Task 4 - Analyze network properties (1.5 person month) (Section 2.4)
- Task 5 - Prediction of transaction fees (1 person month) (Section 2.5)
- Task 6 - Privacy implication of bloom filter based SPV wallets (1 person month) (Section 2.6)

5.1 Milestones

We consider the following milestones, where the work would cover 6 months overall:

- After 2 months: Have the tool with its basic functions finished, already work on analyzing JoinSplit transactions (Task 2 and 3)
- After 4 months: Finish the work and report on Tasks 2 and 3, already start working on the network properties (Task 4)
- After 6 months: Finish with the remaining tasks, publish the tool and a whitepaper about the project (which would be later submitted to a conference)

6 Budget

Our budget would be 24000$, which would cover around 9 person months of work. However since recommended scale is 1-6 months we can scale down our proposal accordingly. In such case we can implement the parts of the proposal which are seen as the most pertinent by the review committee/Zcash community.

We are also open to collaboration with related proposal number 31 (tried to contact them but they didn't reply so far).

References

BKP14. Alex Biryukov, Dmitry Khovratovich, and Ivan Pustogarov. Deanonymisation of clients in bitcoin p2p network. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, pages 15–29. ACM, 2014.

GCKG14. Arthur Gervais, Srdjan Capkun, Ghassan O Karame, and Damian Gruber. On the privacy provisions of bloom filters in lightweight bitcoin clients. In *Proceedings of the 30th Annual Computer Security Applications Conference*, pages 326–335. ACM, 2014.