Advanced Zcash Blockchain Analysis

CryptoLUX team, University of Luxembourg

1 Introduction

Our proposal is to continue the empirical analysis of the Zcash blockchain. As we have described in our previous results, the t-to-z and z-to-t transactions in Zcash are linkable in a quite large proportion, mostly caused by the requirement for block rewards to be first converted to a z-address. This alone leads to at least 80% of shielded transaction linkability. Considering the previous results, we still have areas, that seem valuable to investigate in detail.

2 Technical approach

As a general goal, we will continue supporting our tool (will be released at the end of June), and update it with the upgrades to the Zcash protocol, mainly concerning the sapling update.

2.1 Mempool

Analyzing the mempool transactions for patterns. We have not examined the mempool of Zcash in detail yet, but it might reveal some crucial usable information for deanonymization. We would also work on optimal transaction fee prediction based on the recent blockchain and mempool information.

2.2 Payment structures

Investigate payment structures both in public and hidden transactions as well. Extend previous payment analysis, look for patterns known from previous works and observations on public chains, and apply them to hidden transactions.

2.3 Further Miner Analysis

Further miner analysis, including the fine tuning of miner linkability and removal of false positives. Finding the marginal miners/pools as well as improving coverage of the history of Zcash (currently 92% for the entirety of the chain, while recent months are at least 95% covered). Continue our work on search of ASIC miners, ASIC miner testing, speed of mining landscape saturation with ASICs, effect of ASICs on GPU-mining profitability.

2.4 Exchanges

Study further the interaction of exchanges with the blockchain. Find more addresses connected to chains and link them, explore what portion of the transactions are connected to exchanges and miners/mining pools, what is the size of the anonymity set of the chain after removing these transactions, how many transactions remain and what are their general use cases.

2.5 Hard-Core Shielded Transactions

Analyze the remaining 2,000 unlinked joinsplit transactions per every 10,000 blocks, can these still provide some extractable statistical information? Explore other linkability approaches, for example the change of old-style Sprout notes into new-style Sapling notes. Investigate the false positive rates for the existing heuristics.

Active attack approaches Majority of blockchain analytics involves passive study of past blockchain data, the topic of active attacks is relatively unexplored and is of special interest in the case of privacy-minded coins with a mix of public and private transactions.

Shielded Ecosystem Analyze recommended best practices (schielded ecosystem) provided by the Zcash developers. Suppose one uses these suggestions, can one still deanonymize these transactions, if a specific use-case involves traffic to t-addresses.

2.6 Other Zcash-related Currencies

If the community finds it useful, extend previous analysis and heuristics for other Zcash based currencies (ZenCash, Zclassic, etc.). It could be interesting to explore the forks of Zcash whether they have similar issues, what are their general network characteristics. What is the effect of the additional features that some of them have.

3 Team

The team that would work on the project would consist of PI Alex Biryukov and his PhD student Daniel Feher. We might use expertise from other members of the CryptoLUX team if necessary.

4 Ethical 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 our previous research on Zcash and other privacy related topics.

5 Schedule

The project would take 9 person months of work, which are divided in the following way and order:

- Task 1 - Update and Maintanance of the Blockchain Tool - 1 person month (Section 2)
- Task 2 - Mempool Analysis - 1 person month (Section 2.1)
- Task 3 - Payment Structures - 1 person month (Section 2.2)
- Task 4 - Further Miner Analysis - 2 person months (Section 2.3)
- Task 5 - Exchanges - 1 person month (Section 2.4)
- Task 6 - Hard-Core Shielded Transactions - 2 person months (Section 2.5)
- Task 7 - Other Zcash-related Currencies - 1 person month (Section 2.6)

6 Deliverables

The project would result in a whitepaper with our findings (which would be later submitted to a conference). The set of tools for advanced Zcash blockchain analysis will be open-sourced.

7 Budget and justification

Our budget would be 18,000 USD , which would cover around 9 person months of work and any additional associated cost that would arise. The duration of the project would be 6 calendar months. 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.