Blockchain Analysis using Attribution Techniques

1 Introduction

- What is the topic of this paper and why do I write about it?
  - Tracing Bitcoin users
  - Criminals still utilize Bitcoin

2 Related Work

- What did others do in this area and what were the results?
  - <See paper research>

3 Yet another Blockchain Analysis Tool?

- Why do we need another blockchain analysis tool?
  - Existing ones minimize false negative rate
  - Target customers are different
  - Closed source is not an option

4 Criminal Prosecution Context

- What are the pitfalls/specialties in the context of criminal prosecution?
  - Users are not “normal”, they try to hide
  - We can access _some_ private information
  - Private institutions must not work as investigators, but analysts

5 A Word on: Machine Learning and Attribution

- What are the pitfalls of machine learning and attribution?
  - Not knowing about the model is really bad
  - Important decisions should be based on profound understanding

6 Redefining the Problem

- What is the exact problem I try to solve?
  - Finding users that try to hide
  - Use only blockchain analysis (not network analysis)
  - Where did coin XY go to?

7 Finding Features

- What features can be found/used to identify individuals?
  - Time based
  - Amount based
  - Transaction shape based

8 Making a Decision

- Why do I use a majority vote?
  - We are talking about evidence, not proof

- Results can be interpreted more easily

9 A Word on: Probabilities

- How to properly interpret probability scores?
  - The final scores only tell how many of the more or less equally weighted clues hint towards the declared outcome
  - More exact statements are difficult, if not impossible (example)

10 A Proof of Concept Implementation

- What is and what is not part of the PoC implementation?
  - Feature set description
  - Stating the problems of bit data on limited resources

11 Evaluating the Scheme

- How was the approach evaluated and what were the results?
  - Describing the “gold standard”
  - Describing the scores
  - Describing the scheme

12 Case Study: ToDo

- Can the approach survive in the wild?
  - Apply it to a real world scenario (omit if time runs short)

13 Future Work

- What needs to be done in the future?
  - Improve “gold standard”
  - Implement more features
  - React to the ever-changing world ;)

14 Conclusion

- What lessons have I learned?