Towards Implementing a Crypto Currency Flow Analyzer for Law Enforcement Agencies

Degree programme: Master of Science in Engineering | Specialisation: Information and Communications Technologies
Thesis advisor: Prof. Dr. Ulrich Fiedler
Expert: MLaw Mike Kindler
Industrial partner: Law Enforcement Agency, Switzerland

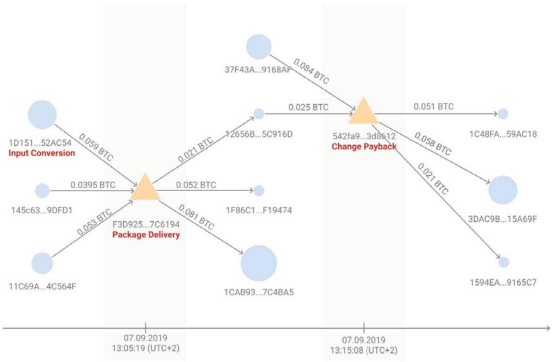
Law enforcement agencies struggle with the complexity of cryptocurrency crimes, since appropriate means of investigation are not available. If agencies had access to a visualization tool, they could explore and document the cryptocurrency transactions efficiently. In this work we demonstrate a visual presentation of Bitcoin transactions and present a software solution for efficiently working in cryptocurrency crime cases.

Initial Situation

Crime scenes are increasingly situated digitally in the internet. The seizure and subsequent investigation of evidence often reveals digital traces that lead to cryptocurrencies such as **Bitcoin**. Past cases have shown that the complexity of cryptocurrency investigations is often so high, that investigators had to use hand drawn visualizations to keep track of all relevant activities. However, focusing on the interesting activities and suppressing the irrelevant data is nearly impossible. If investigators had access to an **automated visualization**, they could find the relevant activities efficiently and document the results for use in court.

Approach

In collaboration with a law enforcement agency we planned, designed and built an application that visualizes Bitcoin transactions. Since the requirements were initially unknown, we first developed the visual presentation, elaborated a systems- and screen-design and built a **minimum viable product**. Afterwards, we collected feedback from the investigators and conducted a **field-test**. We have then realized the improvements in an iterative process by working in three-weekly sprints. As a result, the agency could continuously influence the improvement process.



Example visualization of two Bitcoin transactions

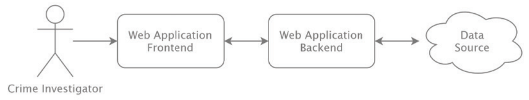
Results

Our solution is a **web-accessible visualization tool** based on a graph. Investigators can visualize Bitcoin addresses and transactions, annotate elements, show additional details and export a PDF report. The proposed graph is aligned on a horizontal timeline, preserving the aspect of time, so that investigators can quickly locate all transactions in the relevant time frame. Furthermore, an automation process allows finding related addresses and transactions in the neighborhood so that new traces such as pyramid schemes can be discovered.

The data used in the visualization is retrieved from a publicly available web service. A **backend** component abstracts the data and provides an API and WebSocket endpoint used by the frontend. The **frontend** component then presents the visualization to the user. In our tool we developed a custom algorithm for calculating and drawing the graph, as existing solutions were insufficient. Since we containerized the components, the tool can be easily distributed to other law enforcement agencies.

Outlook

By having access to a visualization tool, law enforcement investigators can now find the relevant Bitcoin activities **more efficient**. The tool fits well into the existing law enforcement process, as documenting the results found by investigators is a key aspect. In the near future we will improve the tool by supporting more cryptocurrencies and integrating available databases for identifying and clustering wallets. We will also setup a platform **shared with other law enforcement agencies**, so that the tool can be used by other cantons and external feedback can be gathered.



System Components

Florian Andreas Bühlmann
f.buehlmann@gmail.com