Blockchain Project - Group 8

Timing Analysis of Monero Transactions using a novel Transaction Explorer

Privacy is one of the most attractive things about cryptocurrencies. It is well known that Bitcoin does not provide absolute privacy that some desire. Even for normal users, the lack of privacy might have an impact. Since the origin and ‘life’ of a Bitcoin are all presented out in the open on the blockchain, Bitcoins can be ‘tainted’. Tainted bitcoins are Bitcoins that were part of illegal activity sometime in the past. Monero, which finds its origin as a fork of Bytecoin, solves these problems. Our project focuses on whether this is actually the case, or in short, how much privacy can Monero guarantee?

Goal

The introduction briefly mentions the question we would like to answer in this report and with our product. Though the question seems rather straightforward to answer, the truth is of the opposite nature. To ensure we are able to deliver a product which is of sufficient quality we will set out the scope of the project. For this reason, we limit the project in size.

We know that the ring signatures of Monero on their own are shown to be ‘perfectly secure’. Once we have additional information about this signature it gets more tricky. Monero can no longer guarantee the anonymity of the transaction due to this leak of information.

While this fact is known, both in the Monero community and by its creators, we want to further develop this concept. To this extent, we strive to develop a tool that visualises the relationship between transactions and their components. Most prominently we want to feature the public keys of Monero. Since the ring signature's safety relies on using multiple public keys available on the blockchain, we want to visualise data available such that it is easy to acquire new insights based on data distribution.

Visualisation

The main focus of our project is finding a way to effectively visualise the transactions in the Monero blockchain. More specifically, we want to ensure the relation, based on the public keys, is properly displayed. This concept brings us to the very first concept of our design and visualisation, the *inter-relational transaction overview*. This view provides us with our initial view of a transaction. To stress the relational aspect of the transaction we define the inputs of the transactions and the outputs of the transactions. The overview provides the former on the left side and the latter on the right. On the left side, all transactions for which one or more outputs are part of a ring signature in this transaction. The transactions on the right represent all transactions for which an output of this transaction is an input.

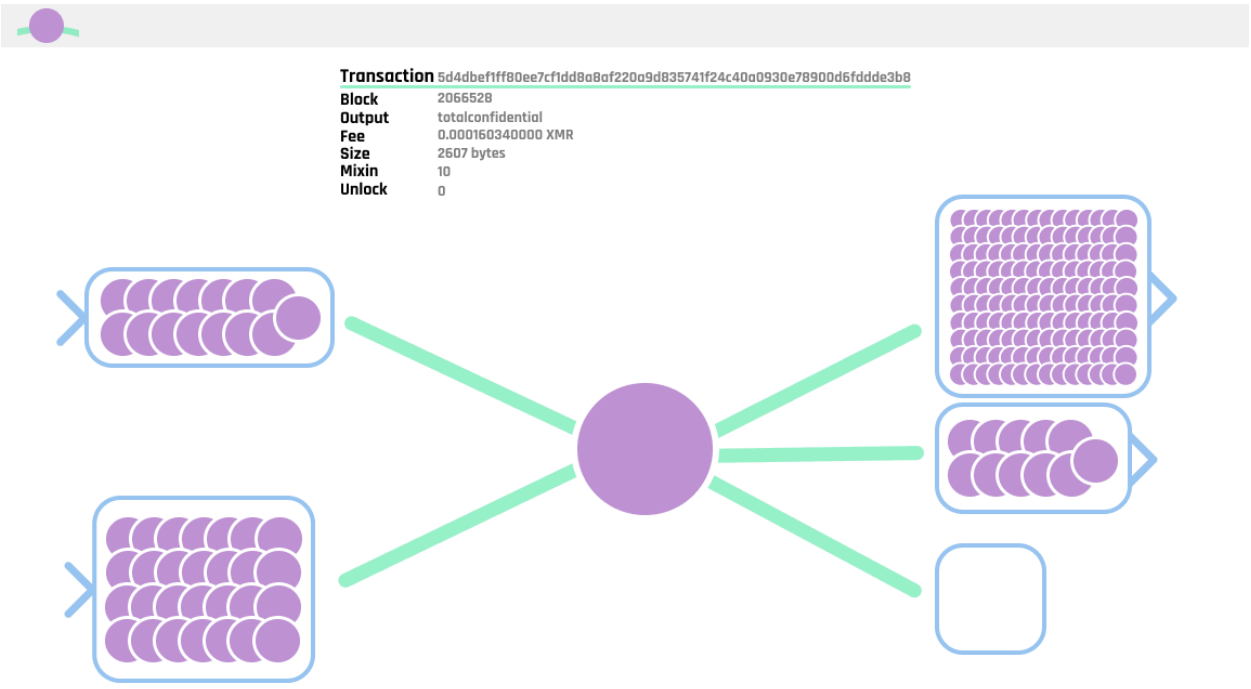

Figure 1: Mock-up for the inter-relational transaction overview

This overview serves as a basis for our *transaction anatomy view model*. The anatomy of a transaction is quite simple, it has one or more inputs, an amount of XMR that needs to change owner (public address), and one or more outputs. The previous overview serves as a basis for our model because it provides the origin of our inputs and the uses of our outputs. However, there are more layers to our model. As one can imagine knowing the origin of the public keys is useful, but we want to make sure the public keys themselves are also part of the product we are creating. This brings us to the *intra-relational transaction overview*.

The aim of this overview is to provide a user with all the necessary information that is specific to the transaction currently selected. The figures in this document represent the same transaction. From what is available in both figures we see that 15 origins provide one ring signature with outputs and 28 do so for another ring signature. The unique element on the intra-relational transaction overview is the graph at the bottom. This plot provides the aggregated timeline of used public keys. This concept is later discussed in more detail.

The combination of these two overviews provides a novel way of discovering the Monero blockchain. This newly found way can be of assistance in examining the Monero blockchain and searches of abnormal transactions.

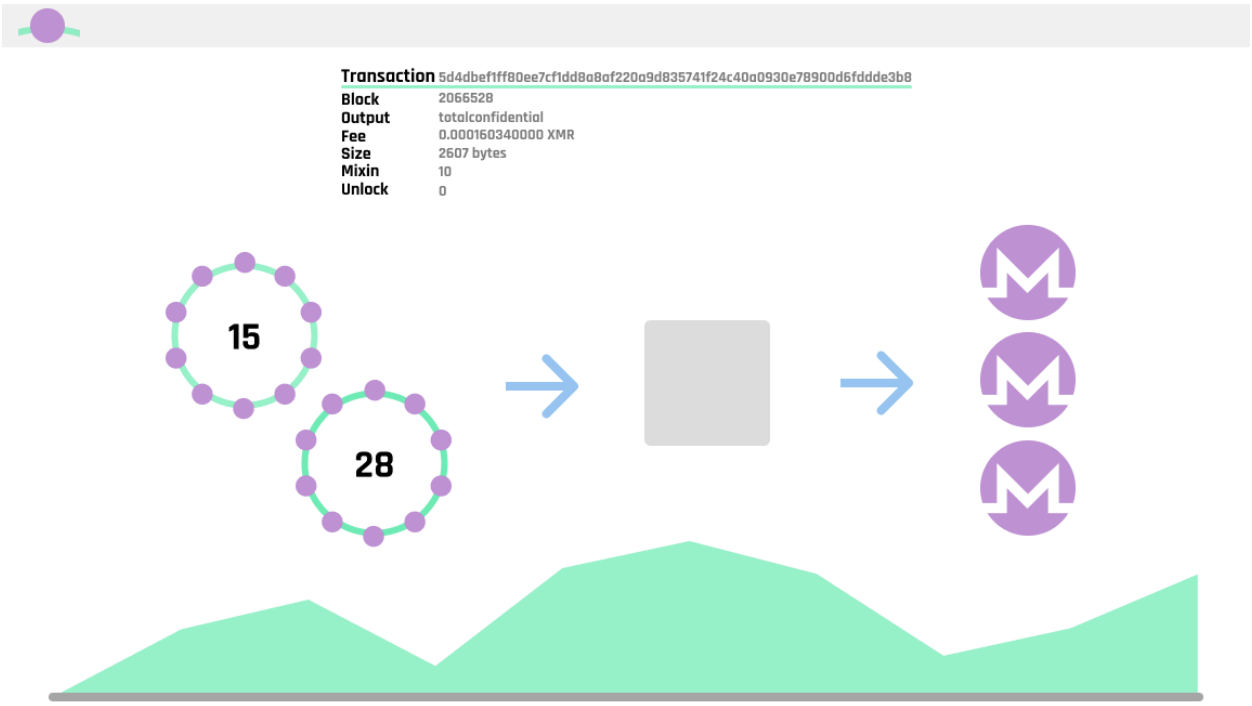

Figure 2: Mock-up for the intra-relation transaction overview

Time as a component

Analysis over time provides us with much more information regarding the users of Monero. A transaction on its own might not reveal information, but multiple over time can. For example, a simple attack could be a combination of factors which result in unravelling the chain and determining which input is actually spent. Such an attack could be executed as a 0-decoy vector with a chain reaction[1]. The intent of our block explorer is to provide multiple attack or analysis vectors so exploring the Monero blockchain becomes easy. This can provide insights which might otherwise be obfuscated. However, to appropriately scope the project our proof-of-concept will focus on anomaly detection over time.

Generally, it is more likely one spends a new Monero over old Monero. This means that overall the expenditure graph of a transaction should be biased towards the present. The visualisation we add in our proof-of-concept is an aggregated date graph of all inputs. Meaning, we gather the transaction dates of all inputs recursively and plot this in an easy overview of the main information page for a transaction.

This addition of extracted and aggregated data provides unique opportunities for anomaly detection within a block explorer. For our proof of concept we used two recursion steps and

[1] For a concrete breakdown of this attack or other known vulnerability check out the ‘Breaking Monero’ series on YouTube.

aggregate all the dates at which the inputs were created. Next we apply a technique called Gaussian smoothing to create a line graph representing the probability density function underlying the data. We chose this form of smoothing because it fits its line according to a normal distribution which is the best alternative for unknown data due to the central limit theorem.

This probability density function is finally plotted on the transaction page and represents for any given point in time the likelihood of an input of this transaction originating from that point in time. This could finally be used to perform anomaly detection and find odd transactions.

Prototype and possible use cases

Although the current implementation is still very much a prototype, one can see the possible use cases. The prototype can be found at http://explorer.bct.diederik.it/ . A very normal, modern (thus with all current privacy methods enabled) transaction can be found in figure 3 (and at http://explorer.bct.diederik.it/#/transaction/2f9d05dc8c2f5efa41dd72995a454bc151133108ae1138ad19e87e2c4bec6ee6).

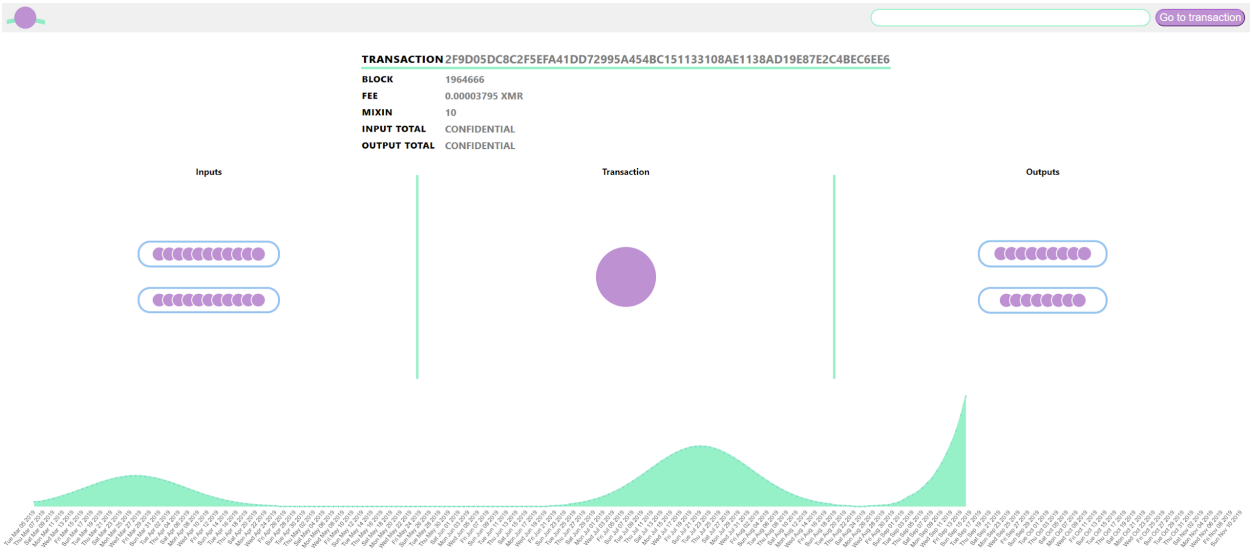

Figure 3: a normal transaction

Notice the input pattern at the bottom, where all inputs are from recent transactions. The far left of the graph is 05-04-2019. Abnormal transactions might look like figure 4, where there clearly is a different pattern at the bottom. The input transactions are way older than in a regular transaction. This particular transaction doesn't hide its amount and was worth about $630 000 at the time.

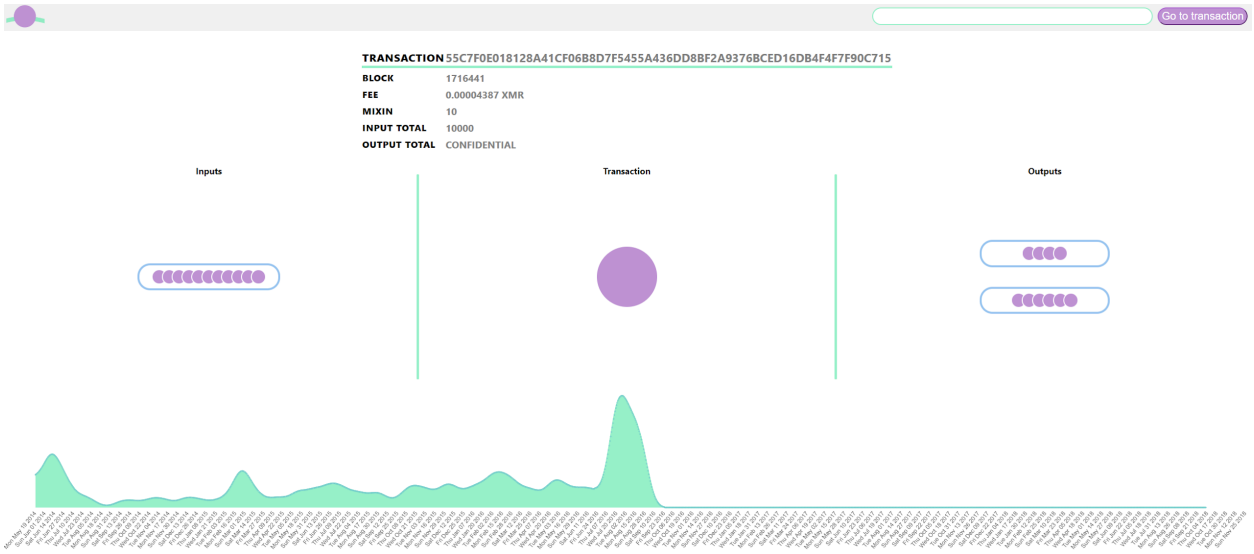

Figure 4: a suspectful transaction

Conclusion

In this short report we provide a general overview of a novel Monero blockchain explorer. The explorer focusses on transactions and the relations between them. The focus of inter-relational transactions allows users of our platform to emerge themselves into the world of Monero. Monero is focussed around privacy by obfuscating input, encrypting outputs, and stealth address to transfer to. However, the level of privacy decreases when we have more data, or in other words, when we combine the transactions. This is why we introduce visualisation and data aggregation as a central part of our explorer. Not only do we stress the relational component of Monero and blockchain using a visualisation based on graphs, we strive to introduce heuristics to analyse the origin and nature of transaction.

Summarizing we introduce a new blockchain explorer that combines all information available. This is reflected in a proof-of-concept that shows the potential of the explorer.