

Empirical analysis and technical feasibility study of crypto-accounting

Thomas Liebberger, Bachelor Business-Informatics, Supervising professor: Prof. Dr. Junker-Schilling

I. CURRENT SITUATION

As the popularity of crypto currencies increases, so does the interest in using them in the business environment. This is particularly evident from the current market capitalisation of all crypto currencies of \$208,749,889,618 (October 2018). Due to blockchain specificities in the way transactions are handled, it is not possible for users without in-depth knowledge to retrieve the data from the blockchain in such a way that relationships between transactions can be identified. Transaction history is not encrypted in most public blockchains. It is freely accessible to everyone. This is one of the basic principles of Blockchain technology. The common clients however, do not offer the possibility to perform historical searches for specific addresses without scanning the entire Blockchain. Such a query on a bitcoin node takes seven hours at the present time in October 2018. Queries of this type however represent the technological basis for enabling real time applications such as accounting or forensic analyses. In a company in which several thousand transactions are carried out daily, it is not possible to track the payment flow without programming effort of one's own. In addition, if using a HD-wallet, which corresponds to the standard, a new address is used for each transaction. Compared to conventional bookkeeping, this would mean opening a new bank account for each transaction. However, companies that have to handle crypto payment flows have a great interest doing this without great effort.

II. OBJECTIVE

It is intended to present an overview of the scientific studies in the field of crypto-accounting that have been carried out so far. Additionally, not only the results of current scientific research studies will be presented. Rather, current methodologies can be discussed on how crypto-accounting is implemented in reality. Furthermore, the technological point of view is considered to clarify how to drastically reduce access times to transaction history from the point of view of addresses. Based on the findings and methodology, hypotheses can be derived for my own empirical research and show whether improving response times to address searches is sufficient to provide a solid, resistant and reliable fundament for crypto-accounting. The objective of this bachelor thesis is to develop a prototype which reduces the query response time and handles all issues related to the proper accounting of crypto currencies.

III. APPROACH

First of all the differences between classical accounting and the accounting of crypto currencies have to be shown. In

particular, the type of goods to which crypto currencies can be assigned and the resulting challenges. Due to the fact that the total balance sheet of an address must be calculated on the distributed ledger blockchain, the main focus is to develop a prototype that is able to calculate these as fast as possible, with today's technical means. The data required for this has to be prepared in such a way that it can also be used for search queries for addresses of any number. Therefor the scripts which represent the core functionality of transactions have to be analysed. First the Bitcoin protocol will be investigated. In the following, Bitcoin derivatives and their differences of the scripts described. The prototype has the claim to provide a solid basis for crypto accounting. Accordingly, the state of the art in the field of crypto accounting has to be clarified. The object of consideration are the data to be generated by the prototype in order to derive a suitable data scheme. It is planned to write the prototype in the programming language JavaScript. In order to shorten the time for search queries, improvements can be achieved in three different points:

Read and write operations on the database, code runtime and data communication between the blockchain node and the prototype.

It can be assumed, for a search query, that the operations on the database and the data communication take the most time. For this reason, the fastest working database is selected from existing tests and an optimal caching procedure is being used.

REFERENCES

- [Antonopoulos 2017] ANTONOPOULOS, Andreas M.: *Mastering Bitcoin: Programming the Open Blockchain*. 2. Edition. O'Reilly Media, Inc., 2017
- [BitcoinProject 2009] BITCOINPROJECT: *Developer Guide*. 2009-2018. – available online at <https://bitcoin.org/en/developer-guide#block-chain/>; (last retrieved 03. June 2018.)
- [Dai u. Vasarhelyi 2017] DAI, Jun ; VASARHELYI, Miklos A.: Toward Blockchain-Based Accounting and Assurance. In: *Journal of Information Systems* 31 (2017), Nr. 3, 5-21. <http://dx.doi.org/10.2308/isis-51804>. – DOI 10.2308/isis-51804
- [Nakamoto 2008] NAKAMOTO, Satoshi: *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. – available online at <https://www.blockchain.org/blockchain.pdf>; (last retrieved 31. März 2018.)