How does the money flow? Quantitative techniques for gaining insight into virtual currency systems.

Bernhard Haslhofer
AIT - Austrian Institute of Technology
Vienna, Austria
bernhard.haslhofer@ait.ac.at

Presentation type: Research Contribution

Short CV: Dr. Bernhard Haslhofer is working as a Data Scientist at the Austrian Institute of Technology. Previously, he was an EU Marie Curie Fellow at Cornell University Information Science and a PostDoc at the University of Vienna. His research interest lies in finding quantitative methods for gaining new insights from large-scale, connected datasets, and to develop novel tools to make datasets and analytical procedures accessible and usable in various multidisciplinary settings. At the moment, he is investigating anomaly detection techniques for virtual currency transaction graphs, such as Bitcoin.

Abstract: Recent years have been marked by the rise and increasing popularity of virtual cryptocurrencies, such as Bitcoin. They can be regarded as disruptive innovation challenging the global economic order and having the potential of transforming financial industry practices and existing monetary policies. However, virtual currencies are not yet fully understood and pose a number of research questions across fields. The *block chain*, which is core component of cryptocurrencies, is a publicly available transaction dataset that could help answering such questions. This talk will introduce cross-disciplinary challenges of virtual currency systems and focus on quantitative techniques for gaining insights from the block chain. It will conclude with an outlook on future research perspectives.

Extended Abstract

Recent years have been marked by the rise and increasing popularity of novel virtual currencies, which are also known as *cryptocurrencies*. Bitcoin, which has quietly launched in 2009 (Nakamoto, 2009), has now emerged as the most successful cryptocurrency in history (Clark et al., 2015), with a daily transaction volume already exceeding those of established payment networks (Statista.com, 2013).

Bitcoin is money that is only exchanged electronically and has the same properties as traditional fiat currencies: it has a currency code (XBT), a currency symbol (B), and an exchange rates to other currencies. It also fulfills common functions of currencies, such as measuring value, serving as a medium of exchange, or storing value. However, in contrast to fiat currencies, Bitcoin is a virtual currency system "*without any trusted parties and without pre-assumed identities among participants*" (Clark et al., 2015). Instead, money issuance and transaction processing is entirely handled by participants in a distributed peer-to-peer network and a consensus protocol strongly relying on asymmetric cryptography.

A core constituent of Bitcoin and other cryptocurrencies is the so-called *block chain*, which is a publicly available ledger of all transactions ever processed by the Bitcoin network. It is organized as a sequence of *blocks*, where each block contains a list of *transactions* and a hash over the previous block, which makes already processed transactions immutable. Each transaction records a transfer of currency units from one Bitcoin address (e.g., *1MuSWqHzrtHmSGHEuvj3N41SWv1dpf9zQV*) to another, where addresses are hashes of public keys, which are in possession of no further defined entity.

Bitcoin and its underlying conceptual and technical design can certainly be regarded as disruptive innovation having the potential of transforming the financial industry and existing monetary policies. However, virtual currencies are not yet fully understood and challenge established perceptions and models of monetary systems and existing policies and regulations. From a technical perspective, questions such as scalability, long-term stability, and security of distributed cryptocurrencies such as Bitcoin "*are currently defined in many vague and sometimes conflicting ways, a system which requires further investigation*" (cf. Clark et al., 2015). The block chain, which also represents a publicly available dataset of all transaction ever processed within a monetary system, offers novel opportunities of answering such questions by applying quantitative analytics techniques.

The goal of the proposed talk is to first introduce the conceptual and technical properties of virtual currencies. Further, it will outline current socio-economical and technical challenges posed by virtual currency systems and given an overview of quantitative analytics techniques currently in place for gaining insight from publicly available virtual currency transaction data. The talk will conclude with an outlook on future research perspectives in this particular field.

References

Clark, Joseph Bonneau Andrew Miller Jeremy, Arvind Narayanan Joshua A Kroll Edward, and W Felten (2015). "Research Perspectives and Challenges for Bitcoin and Cryptocurrencies.", Technical report. Available at: https://eprint.iacr.org/2015/261

Statista.com (2013): How Bitcoin Activity Stacks Up Against Other Payment Networks. Available at: http://www.statista.com/chart/1681/daily-transaction-volume-of-payment-networks/

Nakamoto, S (2009). "Bitcoin: A peer-to peer electronic payment system." 2013. Available at: https://bitcoin.org/bitcoin.pdf