Explorative Qualitative Analysis of Cryptocurrencies' Potential Risk Factors

Masterarbeit

zur Erlangung des akademischen Grades „Master of Science (M.Sc.)" im Masterstudiengang Wirtschaftswissenschaft der Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

vorgelegt von

Name: Dammermann   Vorname: Vanessa

██████████████   ████████

Prüfer: Prof. Dr. Michael H. Breitner

Hannover, den 27.09.2018

Table of Content

1. Introduction

Since the most popular cryptocurrency was established in 2008, cryptocurrencies are still in the focus of the media and receive public attention in the digital century. Cryptocurrencies became widely known because of their new and innovative technology and decentralised system. They can be described as a decentralised peer-to-peer (P2P) network and contain underlying technologies, such as the blockchain technology. Because of the decentralised nature of cryptocurrencies, no financial intermediary is required for executing a transaction. Furthermore, cryptocurrencies are classified with virtual currencies and they are based on an encryption process, by which a certain privacy level for users exits (see Pak Nian, Lee Kuo Chuen (2015), p. 8). Researchers started to discuss possible advantages of cryptocurrencies, because the popularity and the innovative technological features increased. Therefore, they came to the conclusion, that cryptocurrencies may have the potential to be used as an alternative currency (see Singhal, Rafiuddin (2014), p. 4).

But besides the cryptocurrency hype, different researchers and the practice started to focus on the risk factors of cryptocurrencies. More importantly, researchers look through the security features and the privacy level of cryptocurrencies and search for solutions to manage possible risks (see Karame, Androulaki (2016), p. 2). Considering the security, cryptocurrencies can ensure the integrity, confidentiality and transparency because of their decentralised P2P network and advance technology (see Stamp (2011), p. 8). Despite these pros, there are some errors in the security and privacy of the system, as the transactions are stored and viewable publicly. Also, security issues are a challenge for big exchange companies, other service providers, as well as for people who are involved with the cryptocurrency-world. Hence, cryptocurrencies contain several security and privacy risk aspects which can have an impact on their network and on the users (see Garman, Green, Miers (2016), p. 3).

Furthermore, awareness about security and privacy risks is increasing among the cryptocurrency's audience because of the ongoing digitalisation. A significant amount of people hold a critical position towards the consequences that the errors in cryptocurrencies' system they might face, regarding the data transparency and privacy they are offered (see statista (2018). Additionally, glancing at some of the famous negative historical events like cyber-attacks on cryptocurrency exchanges, people also have in mind the thefts and frauds others have faced dealing with cryptocurrency (see Coppola (2018); Quora (2018)). Also, Bitcoins might be used for money laundering, mining or trading goods on the dark web because of the pseudo-anonymity within the Bitcoin system (see Nica, Piotrowska, Schenk-Hoppe (2017), p. 25; Garman, Green,

Miers (2016), p. 3). Consequently, the question arises what kind of security, privacy and transparency risks cryptocurrencies hold and how the public and participants of the cryptocurrency networks should deal with the risks. Therefore, the following research questions were developed:

What are the information privacy, information security and the transparency risks of cryptocurrencies?

And how can these risks be managed?

As a result, the aim of this work is to give an overview of the information security, information privacy and transparency risks of cryptocurrencies. In addition, the aim is to find solutions for possible ways to manage the risk factors in the future. To answer the research questions, an explorative research methodology to present the scientific view and a qualitative approach by interviewing experts to analyse the practice will be used. Because of the high popularity of the cryptocurrency Bitcoin, this work will primarily focus on Bitcoin. However, further cryptocurrencies with a higher market capitalisation are considered in this work. Furthermore, this thesis mainly focusses on risk factors which concern the user of cryptocurrencies and the public.

The structure of the thesis starts with a theoretical background on cryptocurrencies and definitions about the information privacy, information security and transparency of cryptocurrencies. Following, the main part of the thesis starts with the explorative research and the qualitative research to identify the risk factors and the potential management measures. Afterwards, the results are presented, discussed and compared. Finally, the limitations of this thesis and a conclusion finishes this thesis.

2. Theoretical Background of Cryptocurrencies

In the following section, the theoretical background of cryptocurrencies will be presented. Therefore, cryptocurrencies in general will be defined. Further on, because of the wide variety of different forms of cryptocurrencies, the most popular cryptocurrency Bitcoin and additionally, a selection of further cryptocurrencies will be described. To give a theoretical overview of the technology behind cryptocurrencies, the underlying technological features, like the blockchain technology, will be explained. Finally, the information security, information privacy and the transparency will be defined to give a better understanding of the risk areas which are going to be examined.

which are analysed by the literature or experts, but it is impossible to consider all factors and measures within one thesis or paper.

Fourthly, this thesis only considers the scientific as well as the practical view of experts. For the further research, it could be interesting to focus on the user experience and the user perception regarding experienced risks of cryptocurrencies.

8. Conclusion and Outlook

The aim of this thesis was to give an overview about the information security, information privacy and transparency risks of cryptocurrencies. Additionally, potential solutions for managing the identified risk factors should be examined. To achieve these objectives an explorative research methodology to present the scientific view and qualitative approach by interviewing experts to analyse the practice was used.

The identified information security, information privacy and transparency risk factors include cyber-attacks, security breaches, pseudo-anonymity, traceability, data provision, human failure, concealment of transactions, technical failures, lacking knowledge, missing responsibilities and fraud. These identified risks can objectify the research question of the thesis and shows that cryptocurrencies and especially their infrastructure and systems bear several risks which have to be observed by the users and the people who are dealing with cryptocurrencies.

Furthermore, the identified solutions to manage the risks are maintenance and system improvement, regulation and standards, secure storage, variation of addresses, user authentication and access management, knowledge improvement, privacy coins, cooperation between legislation and technical experts and political openness. Also, the identified solutions can answer the research questions and indicate that there are opportunities to manage the identified risks in the future. But at this point, it should be taken in mind that there are relationships between single management measures. Also, some measures like the implementation of regulation measures partly depends on factors like the knowledge and the cooperation between legislation and experts. Thus, all solutions should be considered while managing the risks

Beside these risks involved with cryptocurrencies and their management measures, barriers can arise through the management of the identified risks. The barriers are the missing professional expertise, conflict of interest, discrepancy between technology and legislation and scepticism. The barriers show that even if risk management is

possible, there still are problems and obstacles which have to be looked at and removed for a successful management of consequential risks. However, in the end it remains uncertain, whether all identified risks can be managed and whether the barriers can be removed.

Recommendations on conducting more research, would be to focus on the effectiveness of possible-measures to manage mainly the security and privacy risk factors. Furthermore, the conflicts between the desired privacy of users and the aspired monitoring of transactions by central authorities would be an interesting research area for further research. For the future, it might be challenging to achieve a high anonymity and privacy level and concurrently to achieve a regulation and monitoring of the network. Further on, the perception of the end-users of cryptocurrencies could be an interesting research field with regard to the privacy and security of cryptocurrencies.