EAI Endorsed Transactions
on Security and Safety
Research Article EAI.EU

A study of user experiences and network analysis on anonymity and traceability of bitcoin transactions

M A Hannan Bin Azhar[1,*] and Robert Vause Whitehead[1]

[1]School of Engineering, Technology and Design, Canterbury Christ Church University, UK.

Abstract

This paper investigates the anonymity of bitcoin transactions and significance of awareness of the technology by bitcoin users, alongside their experiences in tracing transactions. Bitcoin enables users to carry out transactions anonymously with the virtual currency without unveiling where the real-world source of the income has come from. These transactions may occur without revealing locations or any personal identifiable information of the person who is sending or receiving bitcoins. While there are existing surveys which test bitcoin users' awareness of the technology, they do not focus on bitcoin users' own experience using the technology in terms of tracing transactions and use of anti-forensic tools to increase the level of anonymity. This paper reports significance of users' opinions on tractability and anonymity of bitcoin transactions and compares users' viewpoints collected from a survey with experimental findings observed using network analysis tools.

Keywords: Bitcoin, Blockchain, Crypto-currency, Digital Currency, Privacy, Security.

Received on 01 April 2021, accepted on 30 April 2021, published on 30 April 2021

Copyright © 2021 M A Hannan Bin Azhar *et al.*, licensed to EAI. This is an open access article distributed under the terms of the Creative Commons Attribution license, which permits unlimited use, distribution and reproduction in any medium so long as the original work is properly cited.

doi: 10.4108/_____

1. Introduction

Bitcoin offers its users a virtual currency which can be transferred to any bitcoin wallet in the world with little effort and small transfer fees. It allows users to do it with anonymity [1]. Bitcoin wallets and some bitcoin exchanges do not require identifiable information to use them. A bitcoin user does not explicitly require personal identifiable information to perform transactions [2]. What makes Bitcoin anonymous is the lack of accompaniment between the public key and any requirements of identity data [3]. As a result, these functions give Bitcoin its anonymous element. There is a debate that Bitcoin may not be completely anonymous, such cases of accidental disclosure of a person's public key or even voluntary disclosure links identity data with a public key [2]. There is also the choice for bitcoin users to use anti-forensic tools to increase their anonymity. The introduction of "mixing services" or dark wallets allow for multiple people to contribute to a movement of bitcoins, which can expertly disguise a transaction by mixing it with other transactions, and then sending that "mixed" transaction at a different time within that day [4]. This stops analysis being done on the time and amount that was sent on a transaction. In addition to mixing services, the use of a virtual private network (VPN) and a Tor type browser makes it more difficult to track a transaction [1], although it does not make it impossible or a momentous barrier to tracing transactions.

While there are surveys [5][6] which test bitcoin users' awareness of the technology, they do not focus on bitcoin users' own experience using the technology in terms of tracing transactions and use of anti-forensic tools. The survey is used to assist in monitoring bitcoin users' awareness of the main concerns that come with using bitcoin, as well as finding statistical data on the bitcoin users' experience levels and success with tracing transactions. This paper will compare results of the survey with experimental findings using network analysis. Subjective opinions collected from the survey and objective measures from experiments will be compared to

*Corresponding author. Email: hannan.azhar@canterbury.ac.uk