BTCTrackr

Aaron Doll, Shaheed Chagan, Michael Kranch, and Vaidhyanath Murti
{*adoll, schagani, mkranch, and vmurt*}*cs.princeton.edu*

COS 597B Privacy
14 May 2014

Abstract

Bitcoin is the mostly widely known and accepted of a rapid growing set of online, virtual crypto-currency. Many users are attracted to these new crypto currency because of their separation from any sovereignty or single authority. They are also adopting crypto-currencies because they provide pseudonymity or the ability to use as currency without any direct link to a real world identity. Because of this psuedonymity, many users believe they can use freely without risk of tracking or tracing the coins back to their real identity. Due to the public nature of the bitcoin transaction ledge, an individual's spending habits are actually more easily tracked by non sophisticated advisory than more commonly accepted online payment methods like credit cards. Continuing on the work presented in "A Fistful of Bitcoins", this paper revisits the heuristics for identifying a individuals closure, or the subset of link Bitcoin. We then implement these heuristics in a real-time application made open to the public to allow individuals to avoid linking transactions. Finally, we discuss several other related project and future areas for improvement.

1 Introduction

In this section, we present a brief overview of technical aspect of Bitcoin. We then several known methods of linking Bitcoin addresses presented in previous work. Finally, we discuss issue with this methods and the motivation for a real-time heuristic utility.

1.1 Bitcoin

Bitcoin is an experimental, decentralized digital currency that uses peer-to-peer technology to operate with no central authority. Bitcoins are sent from one address to another with each user potentially having many, many addresses. Each payment transaction is broadcast to the network and then included in the blockchain, or the list of all previous transactions) so that the included bitcoins cannot be spent twice.

Talk about transaction ledge

1.2 Current Clustering Heuristics

Heuristic one - all inputs below to same user. Dicuss change address -

1.3 Motivation

All current implementation were isolated in publicly available code but not an easy to use implementation for the everyday user. They were also not in real time and would have to be re-computed for every individual address. Finally, no one previously published or displayed a list of linked addresses. Since the closures for many large establishments are known, all

2 BTCTrackr

2.1 Parser

2.2 Database

2.3 Website

3 Related Work

The initial idea of identifying bitcoin address has been around for quite some time. This idea was first introduced in the original bitcoin paper when noted that you could assume all input addresses belonged to the same individual.

Our system was built as a real-time implementation of the Heuristics described in "A Fistful of Bitcoins" by Sarah Meiklejon etc al.

Bit Iodine is a recently published project out of the . Spagnuolo recently published his project include a front end web service similar our deployment described in this paper.

4 Future Work and Conclusion

References