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-currencies because they are decentralized and separated from any sovereignty or authority. They are also adopting crypto-currencies because they provide pseudonymity - an individual can make online transactions with the virtual currency without any direct link to their real world identity. Because of this psuedonymity, many users believe they can use freely without risk of their expenditures being traced back to their real identity; however, several recent papers on bitcoin transactions increase demonstrate this belief is false. An individual's spending habits are actually more easily tracked by non sophisticated advisory due to the public nature of the bitcoin transaction ledge 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 cryptographically signed by the owner to prevent illegitiment spending and then broadcast across the peer-to-peer network to included in the list of previous transactions (more commonly known as the block chain). Miners are a special type of user that participates in the network. Miners are responsible for verifying the authenticity of an announced transaction based on the previous transactions in the block chain and including that transaction in the next block (update) to the block chain. Once a transaction is included in the block chain, that transaction can not be altered or reversed.

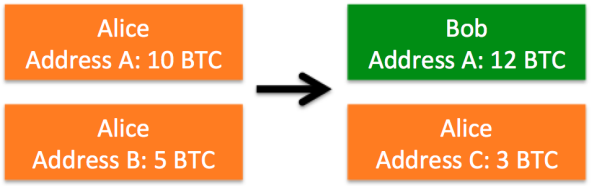

Figure 1: Example Transaction

In the Bitcoin protocol, transactions are simply a list of addresses as inputs with a corresponding list of transactions as outputs. In addition, the sum of all the input address must be greater than or equal to the sum of all the output address with the difference being claimed by the miner (an optional small fee for publishing the transaction). Figure 1 shows an example transaction where Alice pays Bob 12 BTC. Alice uses two address that total to more than 15 address in order to pay 12 BTC. She then pays Bob the 12 BTC and must pay herself back the additional 3 BTC to a third address (commonly called a charge address).

1.2 Address Clustering

.For example, Alice might want to payindividual or entity generally controls many addresses as opposed to a traditional system where a user has a single

account

Te inputs As suggested that transactions In this paper, we refer to the term clustering to mean the group (subset) of Bitcoin address that are controlled by the same individual. Furthermore, we define control as the individual in charge of spending the Bitcoins.

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