Bitcoin Anonymity and The Block Chain

Cian Burns

2014

Masters in Computer Science (MCS)

Supervisor: Dr. Donal O'Mahony

Abstract

Bitcoin is a peer to peer digital cryptocurrency that has risen in popularity in recent times. The Bitcoin protocol relies on a structure known as the Block Chain. This Block Chain is the public ledger of transactions that have occurred over the entire history of Bitcoin and is constantly growing. I will address many aspects of Bitcoin from the history of Bitcoin mining to some in-depth discussions on many of the controversies that plague Bitcoin.

The aim of this dissertation is to demonstrate that by using certain properties of a Bitcoin transaction that it is possible to extract additional information about a user and their addresses from the Block chain. I will discuss the implementation of a system capable of extracting this information and I will also outline the design of a system that would be capable of utilising this implementation to provide a service to both the Bitcoin community and a financial regulator.

As a proof of concept I will demonstrate how using this system it is possible to analyse the actions of a given user. I will use the Bitcoin exchange Mt. Gox as a case study and I will attempt to analyse what really happened to their users missing Bitcoin, by utilising the tools I will create.