VALUE TRANSFER PRIVACY REVIEW THROUGH CRYPTOCURRENCIES

Final Report
by
Tomas Coleman

Student ID: C00218923
Institute of Technology Carlow
Supervised by: Richard Butler
20th April 2019

Introduction

This document will provide an overview of my experience of creating my project. It will cover various aspects, including what was achieved and what is still outstanding, what I would do differently if I was starting over, problems I encountered along the way and what I learned from the experience overall.

Project Overview

This project is about reviewing the privacy of natural humans that have the ability to transfer value between each other. I have gone through and researched all of the technologies that allow a human to do this. I have also researched the laws that are required by different countries surrounding this topic. For example, the laws regarding ‘know you customer’ and anti-money laundering. I have created a demonstration so that I can show that the transfer of value can still be done privately.

The technologies that I used to make the demonstration portion of this project include:

- Monero
- PyQT
- SQL
- monero-python

The tools I used are:

- ILDE
- XAMPP
- phpMyAdmin
- UMLet

What I did right

In this section I will be covering what I believe I have done the correct way throughout this process:

Mastering Monero

I read the book named Mastering Monero written by SerHack, available at: “https://serhack.me/”. This book is the best resource I found while doing this project. It allowed me to learn the majority of what I know about the monero cryptocurrency. This along with the cryptonote white paper allowed me to understand the ideas behind monero and the technologies that it is based on. Its website can be found here: “https://cryptonote.org/”.

Password Management

I have learned from previous projects, this course and from writing the research manual that passwords must be stored hashed and salted for best security practice. I have learned from the research manual that Bcrypt is a hashing algorithm that is designed for passwords. It combines the hashed password with your salt so that it can be put into one column. It also has the ability to increase the work factor as time moves on and PCs get faster.

Deciding on writing necessary classes versus making use of others

I learned as much as I could from the Mastering Monero book and made sure that I understood what the JSON was doing and how it was doing it. I also used this logic to learn about the monero-

python API so that I understood what the methods were doing and what JSON code they were creating.

I made use of the classes that were already written by other people and tested them before using them in my program, as you can never assume that other peoples' code works. I compared this to writing my own code with the time that we have to create this project. I believe I made the correct decision on understanding and using other peoples' code over making my own for these aspects.

Agile development

I am happy that I developed the demo part of the project not as per the waterfall method of software development, and because of this I was able to show people the project earlier and get feedback and fix UIX problems.

What I did wrong

The following list refers to things that I believe I could have done better throughout this process:

GIT

The software version control technology called GIT is widely used to handle the development of software. Based on the problems I encountered regarding backing up and holding different versions of the software for when I wanted to add a new feature, for example the QR Code generate function. I held the working version of the software on different USBs, so that if the QR Code generator made the code unstable, I would have been able to go back to the running version. GIT would have allowed me to backup and manage version control much more efficiently.

Time management

I learned that my time management skills are skewed to work on what I like working on, and that I need to manage them better overall. Take my research manual as an example. I spent too much time on this document in the initial stages, as I am very passionate about what I was learning and writing about.

Address generation

When I was reading through the monero book, I was developing the address generation as that is what I deemed to be the first component that I needed to do. I went ahead and created parts working from a wallet seed before I discovered the monero python API. If I was doing this again I would have spent more of my time at the start looking up APIs before starting to write my code.

IP address leaking

When you broadcast to the monero network you are leaking your IP address which can be used to identify a user of monero, be that they are running a node or transferring value. I am unable to run Whonix, although this would fix this particular issue.

Another way of leaking IP addresses is through malware. We are all human and as such we will make mistakes. One mistake should not allow your entire transaction history to be leaked. The best way to stop this happening is to disconnect the operating system so that if you do make a mistake of downloading malware or a harmful program, it does not have access to your IP address, Qubes OS

is the best way of doing this but because of do not have the appropriate hardware that can run both of these operating systems, I am unable to fix these issues currently.

What I learned from this project

Paper or Cold Wallets

The most secure wallet of all is one where there is no accessibility. An example of this is a paper or cold wallet. This is where a user takes down the keys of their wallet and deletes the wallet off their PC. I have learned about these types of wallets and how they should be used.

Laws

I have spent quite a large portion of the time allocated to this project to learn about the laws that ensure that what I am writing about is legal. The most import parts of this is where different countries have 'know you customer' and anti-money laundering laws, or other pieces of law that enforce different things on businesses or else they would not be able to operate.

Python

At the start of this project, I would not have been able to tell Python apart from any other programming language. To go from that level of knowledge of the language to being completely comfortable with it and preferring it to Java and C is to me the biggest success of this project.

JSON

The monero RPC uses the JSON format. It is extended from JavaScript and is shown in the example below:

```
{"id": "0","jsonrpc": "2.0", "re-
sult": {  "balance": 140000000000, "un-
locked_balance": 84000000000} }
```

In this case, the wallet contains 0.14 XMR, and only 0.084 XMR unlocked.

All of the monero responses are like this and it is very important that I learned how to read and write these.

Achieved

- User interface
- Registration
- Login
- Creating wallet

- Transfer of value

Not Achieved

- Sub addresses

Conclusion

I have achieved the goals that I set out for myself in this project. I have learned so much from this project. It has helped me to greatly understand the world of digital flow of value.

Acknowledgements

I would like to thank Richard Butler for his supervision and for being a great source of knowledge throughout this project. I would also like to thank Martin Harrigan for answering questions I had about the project.

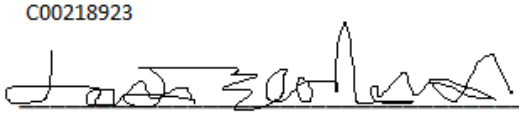
Plagiarism Declaration

Declaration

* I declare that all material in this submission e.g. thesis/essay/project/assignment is entirely my/our own work except where duly acknowledged.
* I have cited the sources of all quotations, paraphrases, summaries of information, tables, diagrams or other material; including software and other electronic media in which intellectual property rights may reside.
* I have provided a complete bibliography of all works and sources used in the preparation of this submission.
* I understand that failure to comply with the Institute's regulations governing plagiarism constitutes a serious offence.

Student Name: Tomas Coleman

Student Number(s): C00218923

Signature(s): 

Date: 29:04:2020