VALUE TRANSFER PRIVACY REVIEW THROUGH CRYPTOCURRENCIES

Research Manual
by
Tomas Coleman

Student ID: C00218923
Institute of Technology Carlow
Supervised by: Richard Butler
1st November 2019

Table of Contents

Abstract

This research manual has been generated along with other papers to answer one main question. Can you get cryptocurrencies from euro and back again, without anyone knowing and in complete privacy? As we move away from physical cash to digital forms of it, as the main means of payment, can we still maintain our privacy. Digital cash is inherently less private as it is always connected to a bank account. The main reason for this is anti-money laundering. Companies in today's world by law are required to implement this in their products to be compliant in other countries so that they can do business in those countries. However, this means that we cannot conduct our business privately. The aim of this project is to find out if we can still conduct our business privately. The answer is yes but like everything in today's world, it is more complicated than a one-word answer. It can be achieved through bartering with cash and gift cards. You must avoid any and all institutions as they all have their relative laws that require them to implement checks that breach your privacy. Why is this question relevant? Why does it matter that someone can see what your spending your money on or, have a say on what you can spend your money on? I believe this is an important part in insuring that we are able to live our lives privately as this is a fundamental right. "In the EU, human dignity is recognised as an absolute fundamental right." (edps.europa.eu, 2019).

Introduction

The objective of this project is both research and implementation. Mainly on *cryptocurrencies, more specifically how someone can transfer value privately, and whether there is any way of getting that value to someone else privately using cryptocurrencies.

The areas that I will be researching will include a combination of the traditional financial world and the *blockchain technologies known as cryptocurrencies. The overall question that I want to answer with this research is whether you can transfer value from one person to another privately without cash being the means of transfer as this has multiple problems associated with it. The order I will go through this research manual is the order that a person would know or unknowingly interact with the technologies as they send a value from them to the recipient. First transforming *fiat in a cryptocurrency then transferring it using a wallet of my design and finally transforming the cryptocurrencies back into fiat if the receiver is unable to spend the cryptocurrency.

Legality

The legality of cryptocurrency has been a question in multiple countries. I have covered this first to ensure that what this paper is covering is legal in the European Union. The legality of cryptocurrencies in Ireland is that initial coin offerings are deemed a "transferable security" and these are dealt with on a case-by-case basis then the existing financial services legislation in Ireland will apply (The Law Library of Congress, 2020). Capitals gain tax will apply to the profits gained from transactions with virtual currencies. The cryptocurrencies that do not get deemed a transferable security are not covered under Irish law (Department of Finance, 2020) The directive (EU) 2018/843 of the European parliament and of the council of 30 May 2018 (Official Journal of

the European Union, 2020) was adopted by the European Parliament on 19th of April 2018 (Jackson, Shah and Hardaker, 2020). It outlines a definition of "virtual currency means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency, and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange, and which can be transferred, stored and traded electronically." This could be confused with electronic money or funds but they are distinct and treated differently. This definition will cover most of, if not all of the existing cryptocurrencies and tokens will be covered by this also. I will not be covering tokens in this paper but they can be thought of as cryptocurrencies that have other tasks or roles then the traverse of value. This amendment extends the scope of *AML directive providers engaged in exchange services between virtual currencies and fiat currencies. The last part of the sentence is the most crucial portion, as only exchanges that are exchanging fiat currencies with cryptocurrencies are required to force their customers to go through the AML requirements. The exchanges that handle cryptocurrencies to cryptocurrencies do not require AML. This also means that exchanges that do not handle the fiat currency and just are handling peoples advertisements as if they were small ads do not have to implement AML. This derivative is also limiting the maximum value of a prepaid card to one hundred and fifty euro this will be a limiting factor but should not stop us from fully completing this project (5AMLD: What You Need To Know, 2020).

Cash to Cryptocurrency

To transform the cash that we have at our disposal into digital means we either need to find someone who is willing to barter cash for cryptocurrency or we can buy mining equipment to mine the cryptocurrency yourself. I will go through buying cryptocurrency first:

Exchanges

Centralised exchanges

There are lots of places that you can buy your cryptocurrencies, centralised exchanges are the most popular but are required by USA and EU law to have *KYC and AML in place to help prevent fraud. This means that the centralised exchanges must take personal data on you to fulfil these requirements. This breaks the privacy of the user which for this project is a fatal flaw. To my knowledge, any centralised exchange is illegal if they do not have these in place.

Decentralised exchanges

The other type of exchange is decentralised. This by law does not have the same requirements as the centralised exchanges because the owners or the people running the exchange do not handle any fiat money, the user does all the handling. A drawback with this is that there will be a log with your *ISP when you log into the website and by your means of payment if it is performed using a digital fiat bank account. This is because your ISP controls the routing of the data that you are sending to and from websites (Know, 2019). To hide this data from your ISP you will need *Tor. This is a web browser such as Firefox, but it must be configured in a different way to hide what you are looking at from prying eyes. Another drawback is that you are putting trust in other person to send you the

cryptocurrencies. You can minimise this risk be reviewing the seller, see what they have done before and see what people have to say about them. You will also need to use cash or a cash transfer method that does not involve tracing who sent the money or who received it. To my knowledge the only ways of doing this are “cash by mail, ATM cash deposits, face-to-face meetings, or gift cards bought with cash” (Localmonero.co, 2019).

ATM

There are ATMs that you can use to withdraw Bitcoin. This has a big advantage as they do not require a sign-up. This is because the KYC and the AML do not apply to them because the cryptocurrencies they use, Bitcoin, “are not legal electronic money” (Bloomberg.com, 2019). They have an upper limit in some countries for a daily transaction (Cash.app, 2019). The main drawback of this method is that their number is very low and the number of the ATMs that allow you to use *altcoins are even lower (Coinatmradar.com, 2019). Another problem with this method is that, to my knowledge, there is no way of getting fiat cash back from these devices.

Mining

Mining is the third and final way to acquire cryptocurrencies. Not all cryptocurrencies use mining but all the ones I will be looking at do.

This is the act of conforming transactions for the market. In doing this you are awarded some of the new coin, though the percentage differs depending on what cryptocurrencies you are mining. To translate the cash into any cryptocurrency, you would have to have PC hardware or an *ASIC. Then you would have to follow the instructions on the website of the cryptocurrency. This is like winning the lottery though, as you are just hoping that you find the hash before anyone else on the network. To be less risky you can pool your hardware with others in a pool. This way you are much more likely to complete the hash before the other people working on it, but you get a fraction of the reward. The advantage of this is you can get cryptocurrencies but without anyone else figuring out that you have acquired the cryptocurrencies.

Proof of stake is a method of conforming transactions by way of using the staked coins as a voting method to validate the new transaction onto the blockchain. By using staked coins which are coins that are not able to be spent by the user. Instead they are kept secured and if the validator, the person that staked the coins approve an invalided transaction, then their stake will be burned and some of the coins will be lost.

In conclusion, using a decentralised exchange or using an ATM will work for this project. To compare the three, mining or staking will require time for your investment of fiat money spent on hardware to return in cryptocurrency. Using a decentralised exchange will only work if there is someone willing to barter with you and give you the right amount that you want. Whereas, an ATM will only work if you are able get to one that is using the cryptocurrencies you want to use and one that is in an accessible range to you. I will pick a decentralised exchange to be used as this has the least amount of drawbacks as there is enough people trying to change cryptocurrencies to fiat and back again that the bartering is much less of a problem than first thought. The ISP problems can be

solved by Tor, and there are multiple ways of getting around the cash only problem caused by the logging of bank accounts.

There are two decentralised exchanges that I have found to be trustworthy. These two exchanges are Localmonero and Liberalcoins.

Localmonero is a web based decentralised exchange. It is very easy to use, and you can browse the market without logging in. It also has a review system so that you can best decide who to barter with. (Dale, 2019) Localmonero has an active community on its forum "https://forums.localmonero.co/" (LocalMonero Forums, 2019).The sites servers are hosted in Hong Kong this has similar law regard a natural person's data as the GDPR in the EU (BitcoinExchangeGuide, 2019a). Localmonero is running Google analytics on their forum and this a very helpful piece of software for the people running their site but it is a privacy breaking feature for us. It can attach your use of this website to your existing profile that Google will have developed on you. This is only used on the forum, but nevertheless, I would encourage the use of their *onion site "http://localmonerogt7be.onion/nojs/".

Liberalcoins is a web based decentralised exchange quite like Localmonero but has more cryptocurrencies on offer. Like Localmonero, you can view traders without logging in, and apart from looks it is very like Localmonero, with Liberalcoins website looking better. Liberalcoins is able to work with multiple altcoins not just Monero, but for this project this is not needed as I will be picking one cryptocurrency. Liberalcoins is based in the isle of man this island has similar law regard a natural person's data as the GDPR in the EU (BitcoinExchangeGuide, 2019b). Liberalcoins does not use any ad tracking software.

In conclusion, I will be picking Localmonero as it has a larger selection of sellers. There is just one for all of Liberalcoins and two for Localmonero just in Ireland alone. I would have a choice of Liberalcoins as it is the better platform as it does not have any social media tags or any Google analytics. Unfortunately this is not feasible with the number of trades available on it.

Comparing cryptocurrencies

We need to be able to transfer our value to another person. That is where cryptocurrencies come in as they allow us to transfer wealth to another person and in the vast majority of cases they are decentralised, but some are more private than others.

Bitcoin

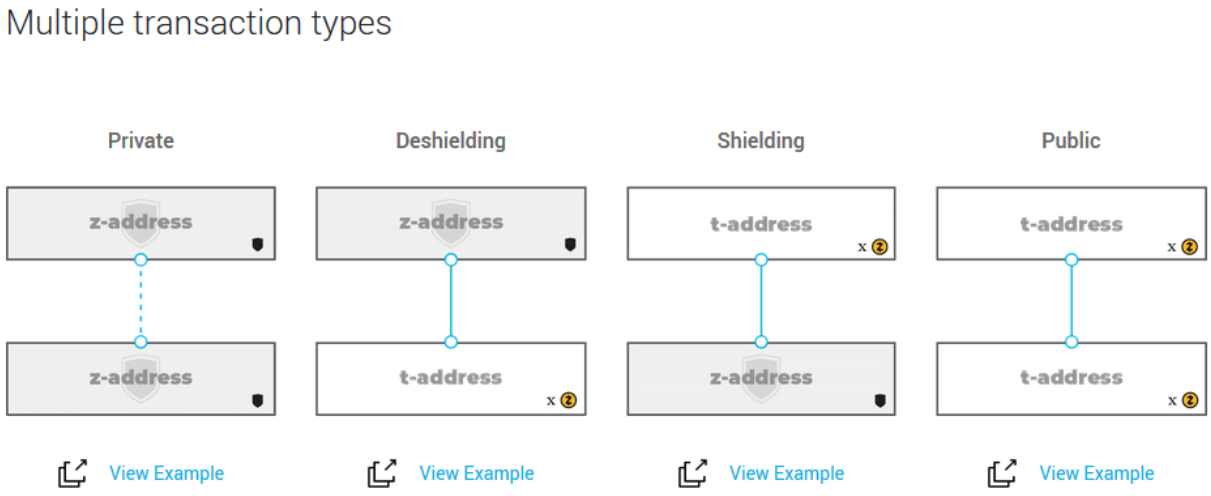
Bitcoin is one of the oldest cryptocurrencies of them all. It uses proof of work. I first thought about doing a Bitcoin wallet for this for its ease of use but there are far too many problems with this cryptocurrency as by its nature it is very open and transparent, because there are no technologies to prevent anyone from figuring out what *address people use, how much was sent, and what the IP address of both the sender and the recipient was.

Zcash

Zcash holds the second highest value of the cryptocurrencies. I will be looking at in this research manual approximately (CoinMarketCap, 2019a) at the time of writhing. Zcash is owned by a company (Zcash, 2019a) called the Electric coin company.

Zcash has tried to be as private as possible but at the same time also trying to keep the amount of data that needs to be put into the blocks on the blockchain to a minimum, because this keeps the *fees that people must pay to a minimum. The fee for a fast transaction in Zcash is .00001 of a coin (BitInfoCharts, 2019). Zcash also tries to take steps towards integrating itself into the financial and banking world by implementing steps that in my opinion, makes the most law abiding or regulation friendly privacy coin.

One of the ways they have implemented this is by allowing the user to have a choice of two types of addresses; T-addresses which are transparent addresses and z-address which are called private addresses.



You can send t-address to t-address, t-address to z-address, z-address to t-address and z-address to z-address, I will go through each one in turn:

T-address to t-address is the simplest. These transactions are totally transparent hence the name. All the addresses and the values that each address has provided are available for all to see using a *block explorer. This type of transaction is call a public transaction.

T-address to z-address is where you can see the *input addresses and the value that the addresses are sending, but not the addresses that are receiving value and how much value goes to each address as these are *shielded. I will cover this later in this manual.

Z-address to t-address is the opposite of the previous transaction type with the actors swapped, so this time the input addresses and the value that each are inputting are shielded but their addresses and their value are not outputted.

Z-address to z-address are the most important for this project because of them being able to shield both the input and the *output addresses.

Next, I will discuss how shielding is achieved through Zcash's implementation of zk-SNARKs:

Zero-Knowledge Succinct Non-interactive Argument of Knowledge (Zcash, 2019b). This allows any person that wanted to prove that the transaction is correct and that no *double spend has occurred in this transaction. This is a lightweight and fast proof as they "can be verified within a few milliseconds, with a proof length of only a few hundred bytes even for statements about programs that are very large" (Zcash, 2019b).

They have wanted to make the proofs as fast as possible. The majority of the time spent on the proof comes from the communication of them over multiple blocks of the blockchain, as either the prover or the verifier should wait for the block to be uploaded to the blockchain, or even multiple block to insure that the communication is on the blockchain and not on a fork or line that would be malicious, and this will add time in multiples of the average block time. Zcash has described this as "non-interactive constructions" (Zcash, 2019b) that "consists of a single message sent from prover to verifier" (Zcash, 2019b). This would make this type of communication take far too long and that can take up too much data in the blocks. Zcash has removed the communication stage and has replaced it with an "initial setup phase which generates a common reference string shared between prover and verifier" (Zcash, 2019b). In Zcash vocabulary this is called a "public parameter" (Zcash, 2019b). If people were able to create these parameters then you would be able to prove transactions that are not in fact valid.

Zcash mining is Proof of Work. It's *algorithm is called "Equihash" (Wilcox and Grigg, 2019). It is based off the generalised birthday problem. This is a theory that states the probability of two people having the same birthday in a completely random set of people increases logarithmically the more

people you add. This is a well-studied problem so this makes this a good base to create an algorithm because it is highly unlikely that this has been misunderstood and could fatally affect the algorithm.

Zcash has the ability for the sender to include “encrypted memos” (Zcash, 2019b). This is only available in z-addresses to z-addresses, also called shielded transactions. This has been implemented in digital fiat banking transactions. According to Zcash’s website, this helps with its USA’s compliance because of the Bank Secrecy Act Travel (Zcash, 2019c), but this rule only applies to transactions “equal to or greater than $3,000 (or its foreign equivalent)”, and ATM and point-of-sale transactions are also excluded (Fincen.gov, 2019).

Zcash allows users that are in control of z-addresses to show others the incoming transactions and memo field for that address but not what address they came from. This does not reveal transaction information for outgoing transactions, but this is a planned development for Zcash. This can be used for law enforcement or for auditing reasoning.

Zcash has implement multi-signature transactions so that multiple people can sign a transaction before it is able to be sent. However this can only be done in transparent transactions and not private or shielded ones.

Zcash has the block size of 2MB and a target block interval of 150 seconds. The simplest transaction type of t-address to t-address takes on average 500 bytes (Explorer.zcha.in, 2019). So that means an average of 26.67 transactions per second. (((2000000/500)/150) =26.67,) but if the block was to contain all z-address to z-address transactions, which average about 2000 bytes (Explorer.zcha.in, 2019), that would mean an average of 6.67 transactions per second (((2000000/2000)/150) =6.67).

In conclusion, Zcash is a private coin that tries to balance privacy, usability, regulation and auditing. This type of balance makes it well suited for users that want to keep their transactions as secure and as private as possible but while also trying to be law abiding citizens. Although the amount of different regulations and compliance issues will mean that it will require a large investment of time and effort to make this cryptocurrency fully compliant. Thanks to its technology, it’s able to keep its fees low and keep the transition speed and the amount of transactions that it can do in one block worth of time.

Verge

Verge is the lowest valued privacy coin at the time of writing. It’s worth 0.003 euro per coin but that on its own does not mean it is the least important cryptocurrency in this manual. Verge tries to maximise its everyday usability both in business and natural persons. It was created under the name of DogeCoinDark (Vergecurrency.com, 2019a). It’s is open-source coin with no main company

behind it, its software is one hundred percent open-source. It also has had no pre-mine, so that the starting contributions have don't have any advantage verses someone that did not invest in the coin before the inception. This shows that the people behind it are not just trying to get the coin some value and then sell all their investment later. This is referred to as a pump and dump scheme.

The main strength of verge is that it uses *I2P and Tor so that it can hide IP addresses of the users of its wallets (Vergecurrency.com, 2019a). This is a very important feature of verge as this is feature anonymises the user of this cryptocurrency.

Verge supports multi-algorithm mining. Verge mining is all Proof of Work. The list of algorithms that verge supports is: "Scrypt, X17, Lyra2rev2, myr-groestl and blake2s" (Vergecurrency.com, 2019a).

Verge has implemented "dual-key stealth addressing" (Vergecurrency.com, 2019a). This allows verge wallets to create one time addresses so that each transaction will be sent to a different receiving address. This is an option and is selected when the sender is creating the transaction.

Verge has encrypted messaging. This is a peer to peer system. This system uses "AES-256-CBC algorithm" (Vergecurrency.com, 2019a). This cipher suite can be broken down into three parts. AES refers to the type of encryption algorithm that is used to encrypt a single block of data. The second part, 256, tells how big the key is. This could be otherwise understood as the password for the block of data. The third section is how the suite encrypts more than one block of data and how the they sometimes linked together.

Verge has plans to implement ring confidential transactions and RSK Smart Contracts. Both will greatly improve verges impact in this space but they are not implemented yet so I cannot include them in my judgement of verge (Vergecurrency.com, 2019a).

Verge tries to insure that the price of its coins stays low so that the coin can be used "in everyday use" (Vergecurrency.com, 2019b). To my understanding, this means that the percentage fee for a transaction when understood in another currency value will not be so large that the person would not make the transaction. There is also no inflation built in to the coin because the total circulation is capped at "16,555,000,000 XVG" (CoinMarketCap, 2019c). The transaction fee for a single transaction is 0.1 XVG (Vergecurrency.com, 2019a). The max transactions per second is "100" (Vergecurrency.com, 2019a).

In conclusion, Verge has implemented many good features to ensure that a person's physical location is not given away because of a leak of IP addresses. Verge has made great work in making it fast and cheap to use. The fee is 0.000334 euro. It does this by insuring the supply is high and by making sure that max transaction per second is high enough and able to grow with the demand.

Monero

Monero is the highest value of all the privacy coins. At the time of writing this is approximately fifty euro per coin (CoinMarketCap, 2019b). This coin has earned a bad name for itself, not through its design but through its uses. Monero has been infamously used in ransoms (Vg.no, 2019) and WannaCry (The Independent, 2019). It is also used for purchasing legal and illegal goods and services. Monero wants to ensure privacy by default. That theory carries through the entire project.

Monero has a large selection of technologies that are all mandatory or as is referred to in the Monero community, privacy be default.

Monero uses Ring signatures. This is a type of *digital signature this allows Monero to hide who sent the value. It works by requiring multiple signatures that are combined into one signature, using the senders own *private key and ten others *public keys. By doing this you can ensure that someone has signed it, but you don't know who (Mastering Monero, 2019a). Monero did not always have these in place. Before 2016, the sender's address could have been identified. In 2016 two or more, 2017 five or more, early 2018 seven or more, and in late 2018 only eleven were made mandatory as if a transaction was to have a substantially higher than average number of keys, then it may be considered suspicious

Monero uses key images. These prove to the network that this transaction has only be done once, as each image is generated uniquely by deriving the actual output being spent and who it goes too (Mastering Monero, 2019b).

Monero uses Stealth addresses. These are one time use addresses that the recipient of the value uses so one is not able to affix anyone to the addresses that is shown on the blockchain (Mastering Monero, 2019c).

Monero uses RingCT, which are "Ring Confidential Transactions" (Mastering Monero, 2019e). This technology conceals the amount of *Moneroj that you send in a transaction. In RingCT there are commitments and range proofs. Commitments are where you commit the amount in a private way, "while not publicly disclosing the amount itself" (Mastering Monero, 2019c) .Range proofs are needed to ensure the commitment amount is greater than zero and less than a certain number. RingCT became mandatory in 2017.

Monero has a technology called Kovri, which is a work in progress and is projected to be finished before the end of this year. This will allow to the hiding of the IP address and physical location attached to that. You can compare this to how verges use I2P and Tor. This will be important to protect the users of this cryptocurrency and the miners.

Monero's algorithm is CryptoNight-R but will change to RandomX after the 30/11/2019. Both of these are proof of work. The fee for a transaction is 0.000039 of an Monero, which is 0.00195 euro and the maximum transaction per second is currently higher than the bandwidth a computer or sever can handle. In most cases, because Monero can scale its block size with the need of its users automatically, and this makes it difficult so say what the max transactions per second would be (getmonero.org, The Monero Project, 2019). There is inflation built in as there is a release of "0.6 XMR per 2-minute block" (getmonero.org, The Monero Project, 2019), wallets that support Monero must enforce.

In conclusion, Monero has some great technologies and a large support community behind it. It has made great leaps forward and continues to do so. It does have the highest fee, but the fee is still very small. It has the best privacy implementation of technology and covers the most bases, which is obvious from just looking at what is done and working and not looking at what is coming down the

line. The one downside to using Monero is that the IP address obfuscation technology is not implemented by default. We can patch this by setting up a VPN on our operating system (OS) of choice.

In conclusion of the cryptocurrencies section, I will be selecting Monero as it has the best setup of privacy protect technologies. I will be creating a wallet to showcase this.

Wallet

The wallet is the main component of my project. It will allow users of Monero to transfer value between themselves without external interference or monitoring. I have multiple choices for how I should design my wallet. The options are CLI, Java's Swing, JavaFX, Python, Tkinter and Python’s QT

CLI is command line interface. This is the easiest way of designing the wallet, as most of the work is done because this is how the original Monero wallet was designed. To my understanding the CLI is hard to understand for non-technical users so that would be a major disadvantage for this style of system.

For the following section I will be splinting the programming languages into closed source and open-source:

Closed Source

Java

While Java is technically open source you cannot re-distribute Java’s development kit and the development model and its governance is not open source. So for comparative sake I will place this language in the close source section.

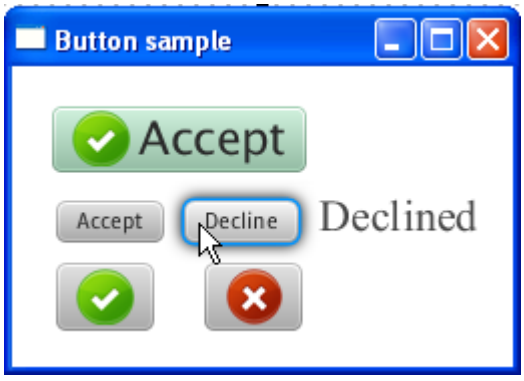
Swing

Java’s Swing is the older of the two Java *GUI’s but this doesn’t mean that it is the least supported. It would be more accurate to say that it is more supported then the newer of Java GUI’s, called JavaFX. Swing is an old-style GUI with very little styling methods other than colour, e.g.

(javatpoint.com, 2019)

JavaFX

JavaFX is the newer of the two GUI's. It adds CSS to its list of capabilities. This makes it both capable of being much more customisable and a lot more difficult to design. It being the newer of the two also means that it is far more likely to have bugs and other issues than Swing has.



(Docs.oracle.com, 2019)

Open source

Python

Python is a fully open source high level language like Java but it does not require any closed source licenses. It was first released in 1991 and was release by Guido Van Rossum but the version that I will be covering will be the latest release version 3.0. This is important as version 2.0 and 3.0 are largely not backward compatible. I have never used Python before and I'm interested in learning it as a lot of my fellow IT students that like to program have talked positively about it.

The two GUI options for Python that I will be going through as part of this research manual are Tkinter and PyQT:

Tkinter

Tkinter is the de facto standard GUI for Python, Tkinter “provides a fast and easy way to create GUI applications.”(Tutorialspoint.com, 2019). This is the easier option as it is the older of the two and will have because of that more answered questions and less bugs.

(Stack Overflow, 2019)

PyQT

PyQT is set of binding in Python that allows it to us QT, which is a C++ framework. It is available in two versions, Qt 4 and 5. From my research QT 5 is very alike to QT 4, as QT 5 is an updated version that works better on mobile devices. It is developed by Trolltect, which is now owned by Nokia. The bindings are developed by Riverbank. I will be using the GPL license for this project but there is a commercial license too. QT comes with documentation that is very good, (Doc.qt.io, 2019) and comes with its own IDE (Qt.nokia.com, 2019).

(YouTube, 2019)

In conclusion I will be using PyQT as there is very little difference and with how QT is used outside of Python I see PyQT as more useful to have in my knowledge base.

Operating system

Next, I looked at which operating system is best to use, as it does not matter how secure our program is if the operating system has malware or is logging data on you. They can be loosely categorised in to Closed source and Open Source.

Closed Source

Windows

This is the most used operating system for desktop PCs in the entire world (Lifewire, 2019). The problem with Windows is that it logs your IP address and other information for Windows to be able

to understand why the device crashed if it does, and what was the device doing that caused it to crash and so on (Hoffman, 2019). This is very helpful from a developers point of view as you can fix problem in your program a lot quicker. This paper is about trying to keep ourselves private and this logging of data will break that privacy. There are many programs that try to ensure that the Windows telemetry is not working (Krishna, 2019). In my opinion Windows also has the most malware built for it and is the main target for virus and malware builders.

Open source

Linux Mint

Linux Mint is one of the most popular distributions of Linux at the time of writing (Distrowatch.com, 2019). It is based on Ubuntu which itself is based on Debian. I have compared Mint to both its predecessors and based on my research, I believe that it is better in all regards. It has more default desktops compared to both predecessors and it very beginner friendly compared to Debian. I also have used Xfce in the past and I find the interface to be the easiest to use. This OS does not have any IP hiding software so I will have to combine this with another operating system running inside a VM on this OS.

Tails

“Tails is a live operating system that you can start on almost any computer from a USB stick or a DVD” (Tails.boum.org, 2019). Tails run all of its network traffic through Tor. One of the design goals of Tails was to “leave no trace” (Tails.boum.org, 2019). This will cause problems with usability as people would have to save any changes and load them every time they start the machine again. This can be undone by telling Tails that you don't want it to be a live operating system and you want it to be saved on a PC desktop and not reload itself, but this is not what Tails was designed to be used as so this will bring its own problems. We will next look at an operating system like Tails but one was designed to be a desktop operating system.

Whonix

“Whonix ™ is a desktop operating system designed for advanced security and privacy” (Whonix.org, 2019). Whonix is also “the only operating system designed to be run inside a VM and paired with Tor” (Whonix.org, 2019). This is the main advantage Whonix has over Tails, because it is always running inside a *VM. This means that the instance of Whonix that is running on the VM does not have access to your real IP address.

Qubes

QubesOS is a security-focused operating system that runs other operating systems in different Qubes. Based on my research this is not a standalone operating system so this cannot be selected on

its own. The major advantage of Qubes is that you compartmentalize your operating system and they have very little control over each other. QubesOS is also not a multi-user operating system.

Virtualisation

I have chosen to use Whonix and not to run Qubes. Because of this, I have to choose a virtualisation software to run Whonix on. There are two choices for this, KVM and virtual box:

KVM

KVM stands for kernel-based virtual and is standard of running VM on Linux machines. KVM is the included in the base for the Linux operating system(Kernelnewbies.org, 2019). The main advantage of KVM is that is fully open and free. One disadvantage of using KVM with Whonix is that they use sparse these are file that add nulls to the end of the file so that the file has room to expand.

VirtualBox

VirtualBox is a free and open-source that is developed by Oracle. It is widely used and is regarded as secure. But not all of the program is open and this is problem with VirtualBox. It calls its self a free and open as the program itself is but if you want the program to do a long list of commonly used features you need to download an extension pack which is closed-source. For example, if you want to use any USB device that is not USB 1.0 or if you want to encrypt your image, then you need to install it (Virtualbox.org, 2019).

In conclusion, I will be choosing VirtualBox only because in the device I will be using to develop this has a 256GB SSD and I am unable to use KVM as the sparse file are taking up too much space. Testing this on another device they are larger than 180GB. Comparing Windows and Mint to, Tails, Whonix and Qubes is not fair to Windows, as Windows has not been designed with the same goals as the latter three. I will be choosing Whonix running on Linux Mint for development as it much more private and has much less logging compared to windows. It is persistent and is best suited to deal with Moreno's main fail, which is its lack of implemented IP address hiding software. For people running the software I will be designing the software to be ran inside a Whonix VM. The program can be ran on Linux Mint but be aware that you will be leaking your IP address. I will have decided that I will be demoing it this way as I don't have two devices that can run Whonix.

Routing

Next I will discuss the options I have with how the device will send the data between itself and the rest of the network. This is one of the most important sections because when you bring accessibility into any setup you introduce the possibility of people being able to gain access to that setup that are not in its physical location.

Tor

All of the operating systems that I have discussed apart from Windows use Tor to route their traffic to their intended target. Windows can be setup but you must configure it yourself. Tor is well documented and is well known. It first came about in 1990 when Roger Dingledine from Massachusetts Institute of Technology. In 2003 the network had about a “dozen volunteer nodes mostly in the U.S., plus one in Germany. (Torproject.org, 2019). It has been an important part of many disclosures, for example Edward Snowden. He showed that the NSA classified Tor as “the king of high-secure, low-latency Internet anonymity” with “no contenders to the throne in waiting” (Armasu, 2015).

I2P

I2P is relatively new compared to Tor, it started as a beta release in 2003 (Geti2p.net, 2019). and is mostly used to access I2P sites. It can be used to access *clear net site, but this is not what it is best suited for.(Cryptocurrency News | Tech, Privacy, Bitcoin & Blockchain | Blokt, 2019)

In conclusion I will be using Tor to send data out to other instances of the blockchain. I have selected this because Tor is more private connecting to the clear net.

Cryptocurrency to Cash

Once the recipient has the value, if they want to transform the Monero back into cash they will need to go through the same steps as they did to get the Monero. Otherwise, they can spend the Monero as they see fit wherever will accept it.

Conclusions

In conclusion, it is possible to transport value using cryptocurrencies, if and only if you are very careful about what you do. The easiest way to do this that I have found still requires more time and effort than using more established methods. Most of my time will be spent on the Monero wallet implementation. We are all only human, so I plan to make sure that it is as difficult as possible for the user to do something wrong that will break their privacy. Taking a leaf out of Monero, thinking of privacy by default and the need for non-technical users to still be able to maintain their privacy.

Glossary

Address: This is where the amount of coins is stored, received or sent from.

Altcoins: This is any cryptocurrency that is not bitcoin.

Algorithm: Software that is used to create the hashes that are used to connect the blocks.

AML: Anti-money laundering. This is commonly tied in with KYC. This refers to having a way of checking where the persons money is coming from.

ASIC: An application specific integrated circuit. A piece of hardware specially designed to do one task.

Blockchain: A blockchain is an append only ledger, a type of list that you cannot delete information from. This type of list contains all its data in blocks that are linked together by having a hash of the block that came before.

Block explorer: This is a tool that is freely available for nearly all cryptocurrencies and allows you to traverse the blockchain for a cryptocurrency.

Clear net: This is any site that does not require Tor or I2P to connect to it.

Coin: If you were to translate this in to normal currencies, it would be the unit of the currencies, i.e. One coin of one cryptocurrency can be understood as one euro.

Cryptocurrencies; A type of blockchain that is where you place value on coins that are recorded using the blocks in the blockchain. There are a few terms that I need to explain so that people can understand this document fully.

Digital signatures: A cryptographic method that confirms the authenticity and source of data or message (Mastering Monero, 2019d).

Double spend: The ability to spend the same value twice, i.e. spending a single euro for two items worth one euro.

Fees: The theory behind these is that the network can sustain itself. The practical side on the other hand changes depending on which cryptocurrencies you are taking about. I will explain how each cryptocurrency implements their fees and what makes each one different and why some charge more than others.

Fiat: This is a type of money that has no intrinsic value but is backed by the central bank of that country.

GUI: Graphical user interface.

I2P: Is a tunnelling service that anonymises data that is sent over its network (Vergecurrency.com, 2019a).

Inputs: The addresses that the value is being transferred from. You can have multiple inputs in one transaction.

ISP: Refers to Internet Service Provider. The business that you connect through to get to the internet. i.e. in Ireland, Eir, Three or Sky.

KYC: Know your customer. This means that must know who your customer is, this usually translates to having a picture and some form of ID.

Moneroj: This is the plural of Monero (Mastering Monero, 2019a).

Onion site: This is a website that can only be accessed through Tor.

Outputs: The address that the value is being transferred to.

Private key: This can be described as the unlock part of the public-private key pair. This is like a digital fiat pin for your ATM card.

Proof-of-work: The idea of that by creating something digital you can prove that a certain amount of work has been done. In cryptocurrencies, this refers to miners having to spend a certain amount of work so as to prove legitimacy of that block.

Public key: This is the public part of the public-private key pair. This is like how an IBAN works for your digital fiat bank account.

Shielded: In Zcash, this means that the transaction information is hidden.

Tor: Known as the onion router. An IP obfuscation service which enables anonymous communication across a layered circuit-based network (Vergecurrency.com, 2019a).

VM: Virtual machine. This is a piece of software that allows a user to run an additional operating system within a device that is already running the operating system that is running the VM.

Bibliography

BitcoinExchangeGuide. (2019a). *LocalMonero – Buy & Sell Monero Cryptocurrency Online/Person?*. [online] Available at: https://bitcoinexchangeguide.com/localmonero/ [Accessed 29 October 2019]

BitcoinExchangeGuide. (2019b). *LiberalCoins – Decentralized BTC Cryptocurrency Trading Exchange?*. [online] Available at: https://bitcoinexchangeguide.com/liberalcoins/ [Accessed 29 October 2019]

BitInfoCharts. (2019). *Zcash Avg. Transaction Fee chart*. [Online] Available at: https://bitinfocharts.com/comparison/zcash-transactionfees.html#3m [Accessed 26 October 2019].

Bloomberg.com. (2019). *Bloomberg - Are you a robot?*. [Online] Available at: https://www.bloomberg.com/news/articles/2019-07-11/bitcoin-atms-show-gap-in-eu-s-money-laundering-rules-police-say [Accessed 29 October 2019].

Cash.app. (2019). *ATM Withdrawal Limit*. [Online] Available at: https://cash.app/help/us/en-us/3086-cash-card-atm-limits [Accessed 29 October 2019].

Coinatmradar.com. (2019). *Bitcoin ATM Locations Worldwide*. [Online] Available at: https://coinatmradar.com/countries/ [Accessed 29 October 2019].

CoinMarketCap. (2019a). *Zcash (ZEC) price, charts, market cap, and other metrics | CoinMarketCap*. [Online] Available at: https://coinmarketcap.com/currencies/zcash/ [Accessed 25 October 2019].

CoinMarketCap. (2019b). *Monero (XMR) price, charts, market cap, and other metrics | CoinMarketCap*. [Online] Available at: https://coinmarketcap.com/currencies/monero/ [Accessed 25 October 2019].

CoinMarketCap. (2019c). *Verge (XVG) price, charts, market cap, and other metrics | CoinMarketCap*. [online] Available at: https://coinmarketcap.com/currencies/verge/ [Accessed 27 Oct. 2019].

ComplyAdvantage. 2020. *5AMLD: What You Need To Know*. [online] Available at: <https://complyadvantage.com/blog/5mld-fifth-anti-money-laundering-directive/> [Accessed 26 March 2020].

Cryptocurrency News | Tech, Privacy, Bitcoin & Blockchain | Blokt. (2019). What Is I2P & How Does It Compare vs. Tor Browser?. [online] Available at: https://blokt.com/guides/what-is-i2p-vs-tor-browser [Accessed 25 Oct. 2019].

Dale, O. (2019). *Complete Beginner's Guide to LocalMonero Review 2019 - Is it Safe?*. [online] Blockonomi. Available at: https://blockonomi.com/localmonero-review/#LocalMonero [Accessed 20 Oct. 2019].

Department of Finance, 2020. *NATIONAL RISKASSESSMENT FOR IRELAND Money Laundering And Terrorist Financing*. [online] Inis.gov.ie. Available at: <http://www.inis.gov.ie/en/JELR/National_Risk_Assessment_Money_Laundering_and_Terrorist_Fi

nancing_Oct16.pdf/Files/National_Risk_Assessment_Money_Laundering_and_Terrorist_Financing_Oct16.pdf> [Accessed 25 March 2020].
Distrowatch.com. (2019). *DistroWatch.com: Linux Mint*. [online] Available at: https://distrowatch.com/table.php?distribution=mint [Accessed 22 October. 2019].

Docs.oracle.com. (2019). *Using JavaFX UI Controls: Button | JavaFX 2 Tutorials and Documentation*. [Online] Available at: https://docs.oracle.com/javafx/2/ui_controls/button.htm [Accessed 29 October 2019].

Doc.qt.io. (2019). Qt 5.14. [online] Available at: https://doc.qt.io/qt-5/index.html [Accessed 19 Oct. 2019].

edps.europa.eu. (2019). *Data Protection*. [online] Available at: https://edps.europa.eu/data-protection/data-protection_en [Accessed 1 Nov. 2019].

Explorer.zcha.in. (2019). *Blocks - Zchain*. [Online] Available at: https://explorer.zcha.in/blocks [Accessed 26 October 2019].

Fincen.gov. (2019). *Funds "Travel" Regulations: Questions & Answers | FinCEN.gov*. [online] Available at: https://www.fincen.gov/resources/statutes-regulations/guidance/funds-travel-regulations-questions-answers [Accessed 26 October 2019].

Geti2p.net. (2019). *Blog - I2P*. [online] Available at: https://geti2p.net/en/blog/ [Accessed 27 Oct. 2019].

getmonero.org, The Monero Project. (2019). *Monero: titles. technicalspecs*. [Online] Available at: https://web.getmonero.org/technical-specs/ [Accessed 29 October 2019].

Herrmann, M. (2020). *PyQT - Python Wiki*. [online] Wiki.python.org. Available at: https://wiki.python.org/moin/PyQt [Accessed 29 October 2019].

Hoffman, C. (2019). *How to See What Data Windows 10 is Sending to Microsoft*. [Online] How-To Geek. Available at: https://www.howtogeek.com/348699/how-to-see-what-data-windows-10-is-sending-to-microsoft/ [Accessed 1 November 2019].

Jackson, K., Shah, B. and Hardaker, E., 2020. *The 5Th Anti-Money Laundering Directive*. [online] Deloitte United Kingdom. Available at: <https://www2.deloitte.com/uk/en/pages/financial-services/articles/fifth-anti-money-laundering-directive.html> [Accessed 25 March 2020].
Javatpoint.com. (2019). *Java Swing Tutorial - javatpoint*. [Online] Available at: https://www.javatpoint.com/java-swing [Accessed 29 October 2019].

Know, Y. (2019). *Your ISP Is Tracking Every Website You Visit: Here's What We Know - Privacy Policies*. [Online] Privacypolicies.com. Available at: https://www.privacypolicies.com/blog/isp-tracking-you/ [Accessed 30 October 2019].

Kernelnewbies.org. (2019). *Linux_2_6_20 - Linux Kernel Newbies*. [online] Available at: http://kernelnewbies.org/Linux_2_6_20#head-bca4fe7ffe454321118a470387c2be543ee51754 [Accessed 19 Oct. 2019].

Krishna, V. (2019). *9 Best Windows 10 Privacy Tools | TechWiser*. [Online] TechWiser. Available at: https://techwiser.com/windows-10-privacy-tools/ [Accessed 1 November 2019].

Lifewire. (2019). *The Beginner's Guide to Operating Systems*. [Online] Available at: https://www.lifewire.com/operating-systems-unix-vs-windows-2180225 [Accessed 1 November 2019].

LocalMonero Forums. (2020). *LocalMonero Forums*. [online] Available at: https://forums.localmonero.co/ [Accessed 1 Jan. 2020].

Localmonero.co. (2019). *How To Buy Monero (XMR) Anonymously (Without ID) Guide - The Most Private Way in 2019 — Localmonero*. [Online] Available at: https://localmonero.co/how-to-buy-monero-anonymously-without-id [Accessed 30 October 2019].

Loc.gov. (2019). *Regulation of Cryptocurrency Around the World*. [Online] Available at: https://www.loc.gov/law/help/cryptocurrency/world-survey.php#eu [Accessed 29 October 2019].

Mastering Monero. (2019a). 1st ed. p.60.

Mastering Monero. (2019b). 1st ed. p.69.

Mastering Monero. (2019c). 1st ed. p.62.

Mastering Monero. (2019d). 1st ed. p.67.

Mastering Monero. (2019e). 1st ed. p.61.

Official Journal of the European Union, 2020. *EUR-Lex - Official Journal Of The European Union*. [online] Eur-lex.europa.eu. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32018L0843> [Accessed 25 March 2020].

Qt.nokia.com. (2019). *www.qt.nokia.com*. [online] Available at: http://www.qt.nokia.com/products/developer-tools [Accessed 18 Oct. 2019].

Stack Overflow. (2020). *Python Tkinter: Attach scrollbar to listbox as opposed to window*. [online] Available at: https://stackoverflow.com/questions/24656138/python-tkinter-attach-scrollbar-to-listbox-as-opposed-to-window [Accessed 1 November 2019].

Tails.boum.org. (2019). *Tails - Privacy for anyone anywhere*. [Online] Available at: https://tails.boum.org/index.en.html [Accessed 1 November 2019].

The Independent. (2019). *Department of Health told WannaCry cyber-attack could have been prevented by 'basic' security*. [Online] Available at: https://www.independent.co.uk/news/uk/home-news/health-department-it-security-wannacry-nhs-hack-report-jeremy-hunt-funding-national-audit-office-nao-a8021881.html [Accessed 28 October 2019].

The Law Library of Congress, 2020. *Https://Www.Loc.Gov/Law/Help/Cryptocurrency/World-Survey.Php#Ireland*. [online] www.loc.gov. Available at: <https://www.loc.gov/law/help/cryptocurrency/world-survey.php#ireland> [Accessed 25 March 2020].

Torproject.org. (2019). *The Tor Project | Privacy & Freedom Online*. [online] Available at: https://www.torproject.org/about/history/ [Accessed 29 Oct. 2019].

Vergecurrency.com. (2019a). [Online] Available at: https://vergecurrency.com/key-tech/ [Accessed 27 October 2019].

Vergecurrency.com. (2019b). [Online] Available at: https://vergecurrency.com/faq/ [Accessed 27 October 2019].

Vg.no. (2019). *Anne-Elisabeth (68) borte i 10 uker – politiet frykter kidnapping etter løsepengekrav*. [Online] Available at: https://www.vg.no/nyheter/innenriks/i/VRnge3/anne-elisabeth-68-borte-i-10-uker-politiet-frykter-kidnapping-etter-loesepengekrav?utm_content=row-1&utm_source=vgfront&utm_term=df-86-sb4f5a82:df-86-sb4f5a82 [Accessed 28 October 2019].

Virtualbox.org. (2019). *Downloads – Oracle VM VirtualBox*. [online] Available at: https://www.virtualbox.org/wiki/Downloads [Accessed 17 Oct. 2019].

Wilcox, Z. and Grigg, J. (2019). *Why Equihash? - Electric Coin Company*. [Online] Electric Coin Company. Available at: https://electriccoin.co/blog/why-equihash/ [Accessed 27 October 2019].

Whonix.org. (2019). *Whonix ™*. [Online] Available at: https://www.whonix.org/ [Accessed 1 November 2019].

Zcash. (2019a). *Privacy-protecting digital currency | Zcash*. [Online] Available at: https://z.cash/ [Accessed 24 October 2019].

Zcash. (2019b). *What are zk-SNARKs? | Zcash*. [Online] Available at: https://z.cash/technology/zksnarks/ [Accessed 25 October 2019].

Zcash. (2019c). *How It Works | Zcash*. [Online] Available at: https://z.cash/technology/ [Accessed 26 October 2019].