International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 4, June 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

The Survey of Transferring Cryptocurrency Anonymization, Privacy, and Security

Vamsi K[1], Ganeshan M[2]

[1]PG Scholar, [2]Assistant Professor,
[1,2]Department of MCA, School of CS and IT, Jain(Deemed to be University), Bengaluru, Karnataka, India

ABSTRACT

The Internet is used in many situations like to send money to a friend or receive money or you might want to buy something, and we're used to using our Visa cards or PayPal or different payment methods in order to transfer money and handle using these traditional methods to transfer money is not anonymous and not private. Therefore, we'll need different methods if we want to protect our privacy and anonymity. You're probably already thinking now of using Cryptocurrencies and that's correct. Some of the cryptocurrencies are actually very secure and very anonymous. So, in this paper I am going to talk about Cryptocurrencies what it is and how it works. We're going to talk about bitcoins obviously because it's the most common Cryptocurrencies. And then we'll also go to talk about a more private Cryptocurrencies which is Monero. So, we're going to talk about how to properly obtain these Cryptocurrencies anonymously and privately how to handle them in a secure and private manner and how to send and receive. So how to transfer these currencies again in a secure private and anonymous manner. In few scenarios in case you needed to transfer money to a friend or to another person in an anonymous manner or if you wanted to pay for something if you wanted to buy something anonymously and privately or if you're simply just buying from a website that only accepts Cryptocurrencies.

KEYWORDS: *Cryptocurrencies, Anonymity, Privacy, Bitcoin, Tails, Electrum, Monero*

How to cite this paper: Vamsi K | Ganeshan M "The Survey of Transferring Cryptocurrency Anonymization, Privacy, and Security" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-4, June 2020, pp.19-25, URL: www.ijtsrd.com/papers/ijtsrd30826.pdf

IJTSRD30826

I. INTRODUCTION

Now in real life you're using cash when you make a payment this payment is processed and is transferred from one account to another using one or more financial institutions or banks. The same goes when you go online and buy something even if you buy with PayPal, Online Banking or some other method. Again, there is usually one or more financial institution to process that payment. So, as you can see this is a centralized structure where one entity is managing payments. And we're also interested in that entity to manage our security the security of our account and our privacy. Now no matter how well you trust this institution or this bank as we seen before centralized structures are just inherently not private. The reason for this is because all of the information is stored in one single place. So even if you trust this company and trust everything about it what about the employees that work at this place. What about hackers that manage to gain access to it. What about other agencies that force this entity to have back doors or to give them access. Simply the idea of keeping everything in one place is not private.

The alternative way to this is to use Cryptocurrencies which is not controlled or managed by a single entity. So previously we had the money which is the cash which is stored in a bank or some financial institution that manages that currency when it comes to Cryptocurrencies. And It eliminates the need to a middleman or to an entity that manages this currency Instead it relies on decentralized peer to peer structure known as blockchain [1].

Now to understand how this works let's have an example where Max wants to send money to Sam to do this Cryptocurrency Network

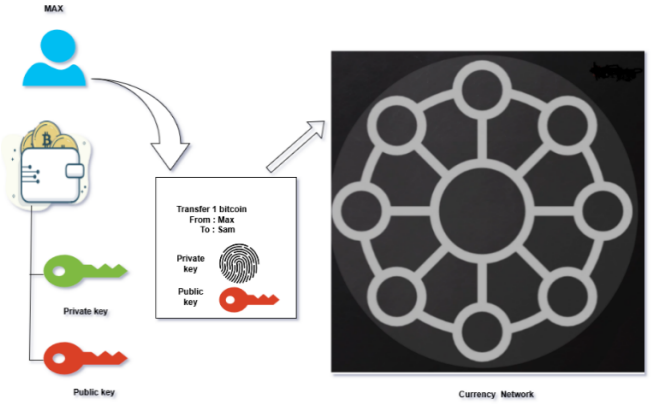

Fig.1. Working of Cryptocurrency Network

At first Max will create a crypto wallet. So, the wallet will be associated with two keys a private key and a public key. And let's say Max wants to transfer one coin to his friend Sam. So, he generates a message or a request, and he'll sign this request with his private key which will generate a signature

or a fingerprint. So again, this is very similar to when we used to sign messages with our private key with PDP[8]. And the reason why this is done to make sure that whoever inspects this message or this request will note that this request to transfer one coin from Max account is actually generated by Max because. Max will never share his private key now once this is signed Max it will also include his public key so that it can be used to verify the signature again. The public key is mathematically related to the private key and therefore it can be used to verify the signature without revealing information about the private key [9].

So, when this message is inspected by anybody, they can use the public key to verify the signature. And if we check it, we'll know that this message was actually come from Max. Therefore, we can send money of one coin from Max to Sam. So once this message is generated on Max and Sam will send this message to the Cryptocurrencies network [9].

Now this network is basically a number of computers usually of high specs that keep a copy of all transactions done using this Cryptocurrencies. These computers are usually referred to as minors because they get paid for maintaining the reports or this record of transactions. Now this record of transactions is known as a blockchain. So, it's a public record that contains all transactions made with this Cryptocurrencies. And each miner each computer on the Cryptocurrencies network contains a copy of all of these transactions [10]. So, it contains a copy of the blockchain. So, Max message is sent to the currency network. It will get verified and if it checks out it will be added to the blockchain. So, this message will be added as a new block to the existing blockchain stored by each one of these computers or miners. Miners will Track every transaction and also Have a copy of the blockchain

So, as you can see this is a decentralized structure. It is not owned by anybody and not controlled by anybody. Anyone can join into this network and use their computer for mining so anyone can download a copy of this blockchain and start mining and start helping maintain this Cryptocurrencies network. In this paper we're transferring one coin from Max to Sam but in reality, real names are not used [2]. Instead of names wallet addresses are used. So, the contents of the blocks even though they're public you'll see the content of it saying it's transferring from an X address to another Y address. And as long as the users are using proper OPSEC keeping their real identity separate from their fake identity connecting using the term network and using all of the tips and methods that we discussed staying private and as anonymous as possible these addresses will not link to their real identities. With that being said the fact that the whole ledger or the whole blockchain is public means that we can read all of the transactions done using this Cryptocurrencies. Therefore, even though these addresses don't link to real identities we can analyse a specific address and see all of the transactions it got involved in, so we can see all of the money that left this address and all of the money that entered this address therefore will even be able to calculate the current balance in this specific account. Now you can obviously just create multiple addresses to get around this. There are also other methods to increase anonymity and privacy and make it hard to see where money is going and where it's leaving from. And you can simply just use a more private cryptocurrency like Monero [11].

Top Best Anonymous Cryptocurrency Exchanges without KYC Verification:

- Binance
- Kraken
- ShapeShift
- Changelly
- Bitcoin ATM
- Monaro

Methodologies to assess Cryptocurrencies in Anonymity, Privacy, Security

Method1: Bitcoin Wallet
Bitcoin is not legal in INDIA The government of INDIA does not recognize bitcoin as a mode of payment I want to walk you through how to use Cryptocurrencies and specifically bitcoins anonymously on the Internet and on the darknet[13].

Now first we have to create a wallet. What we mean by wallet is a software that's going to hold our money in Cryptocurrencies then we can use this wallet to send payments receive payments like a bank account. Now there are a lot of web-based wallets where you can access your currency online using a web browser. There are applications that you can get on your phones. And there are programs that you can install on your desktop computers. Now since we're using Tails Operating System because Tails has a pre-installed application called Electronic[7].

Tails:
Tails is a live Operating System that helps you to use the internet anonymously and circumvent censorship. It is a complete operating system designed to be used from a USB stick or a DVD. It is a Debian GNU/Linux based operating system. It will never use storage of our computer it uses only RAM Memory [8] whenever we Restart our system it shows a fresh operating system. So, if you install external programs, you'll have to install them every time you start Tails unless we use Persistence is enabled So there is an option called Persistence. Persistence helps the user to store their data permanently and it is available for the next time. When the user restarts the Tails, the stored persistent data helps the user for their future use. Persistent drives help to store data like passwords, bitcoins, personal data, browser bookmarks, additional software, network connections etc., this helps the user to access their Tails flash drives anywhere in the world's end-user systems [7]

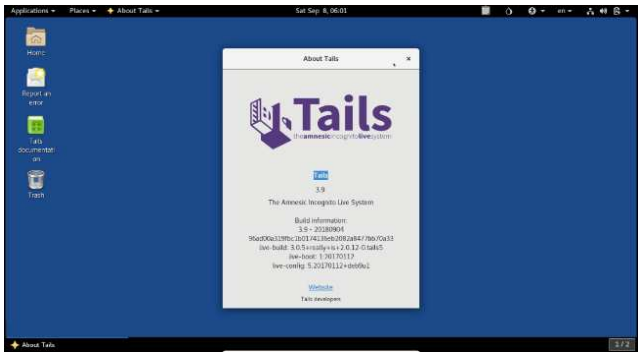

Fig.2. Tails Operating System

Electrum:

The Electrum is a software in Tails operating system it's mainly used for cryptocurrency wallet in a desktop Bitcoin wallet that's available for free download for Windows, Mac, and Linux computers. Electrum is also lightweight Bitcoin client, based on a client-server protocol. The Electrum wallet only supports the storage of Bitcoin. While there are thousands of cryptocurrencies available, Electrum has stuck to their roots by solely focusing on Bitcoin alone to provide a highly secure, fast and efficient Bitcoin wallet. The seed phrase created by Electrum has 132 bits of entropy[8]. This means that it provides the same level of security as a Bitcoin private key (of length 256 bits).

Advantages of Electrum:

- Electrum is software to hold your keys and manage your Cryptocurrencies balance to Receive payments and Send payments.
- It is pre-installed in Tails
- Electrum is it's really fast.
- Fast – no need to download the blockchain
- Account can be used from multiple devices form different places

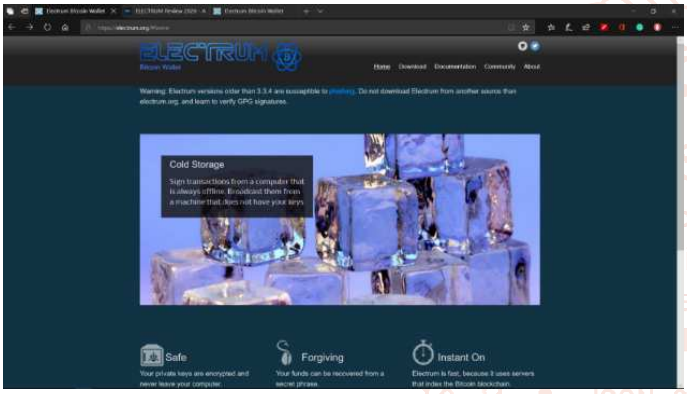

Fig.3. Electum Bitcoin Wallet download page

Installing an Electrum Wallet:

Now to download the latest version of electrons you need to go to their Website electron dot org (or) use this URL: https://electrum.org/#home then select the Linux image and click on Save File and this will automatically be stored in Browser directory. When you download something from the Internet it can be modified, so I'm also going to download the signature. And also download the developer's public. Now we're going to use the public key of the signature to verify that the file has not been modified with since we downloaded it [12].

So now we can run the file because we know the file did not get modified before we do that, I'm actually going to copy this and I'm going to put it in my persistent directory. So, when we create a wallet the wallet information will be stored in this computer. So, when we restart, we won't have to restore the wallet every time [7]. We'll just have to put the password. You'll need to right click the file go to its properties go to permissions and you need to check the box that says allow executing file as program [8]. Now every time you want to run electronic. Don't go to applications Internet com to persistence and double-click this executable. Now as you can see the program has started now.

Fig.4. Persistent directory with Electrum setup

Now that we have our wallets software installed in our system, so we should create our first wallet. So, I'm going to double-click the electronic icon. And we have to create a new wallet. So, the first step to name the wallet that you want to create. Now it's asking us what type of wallet do we want to create by default. This is set to a standard wallet. And this is what we're going to create the wallet with two factor authentication allows you to create a wallet that uses three keys two of which are stored on this computer. And the third is stored on a remote device. And in order to log into this wallet and use it you'll need to use a device with Google Authenticator. Therefore, if you want to be anonymous than standard wallet is a better option than this. You can also create a multi signature wallet. This is basically a wallet that uses two other separate wallets installed on two separate machines. Again, it increases security and because it doesn't require Google Authenticator. So, we're keeping this at standard wallet. We're going to click on Next. Now it's asking us whether we want to create a new seed or a new wallet or restore an existing wallet. A seed is a string of text that can be used to restore a wallet. [12] So, if you already have a wallet on a different computer that you removed or if you already have a wallet that you want to use on this computer then you would select the second option. I already have a seat. If you're a creating a new wallet then select Create a new seed. Then it will ask about Seed type set as Segwit and right now you can see we have our seed. So, like I said the seed is a string of text that we can use to log in to this wallet. So, this is very dangerous. You're not supposed to share this with anybody. If anyone sees this text, they'll be able to log into your wallet. So that's why never store this electronically. You should just memorize it because if anybody sees this string of text they'll be able to log into your wallet and use your money transfer money or receive money now this is very useful for us if we keep it private because we can use this seed to log in to our wallet from different computers or even if we remove tales from here and reinstall it on a completely different USB stick [7].

Now I'm going to copy my seeds and paste it in a Notepad And we're going to click on Next. And in the next window it's literally asking you to paste the seed for verification, and we're going to click on Next. Now it's will ask you to choose a password to encrypt your wallet again use a long and strong password, and we're going to keep this option checked to encrypt the wallet file that will be stored on this computer. Our wallet is successfully completed right now we should check for balance. As you can see, we have zero micro bitcoins because we haven't really transferred anything in here. You we can see blue circle on the right side of the window. If you're not connected then this circle will be red. If you're connected directly it will be green. If you're connected over the Tor network It will be blue. So electoral is just

software that you can install on any operating system and you can see that if you install this on any other operating system other than Tails then you should use Tor. So, make sure that all the traffic that is sent to us from electrons is going through the Tor network first. Now you can also see default in the history tab where you can see all your transactions. You can use the receive tab to get your receiving address and you're receiving QR code you can share them with anybody that you want to receive money. And they will be going to their scent up, and they will either use your receive address or use your QR code to send money to you. Electron is a very simple program that is easy to use its user-friendly.

How to Buy Bitcoin Anonymously?

Now there are a number of ways to buy bitcoins but not all of them are anonymous. To receive bitcoin first we should now our RECEIVING ADDRESS. In our wallet you can see that if we click on the receive, you'll see our RECEIVING ADDRESS. This is the only piece of information that you'll be sharing when you want to receive money into your wallet. And that will be stored in a public ledger in the blockchain. [12]

Fig.5. Receiving Address of the Wallet

Therefore, anybody can come in and analyse the blockchain and see who sent you money. So, if you send money to this address using your bank account or using a service that verifies your identity then your identity will be linked to this address and then any transfer you make from this address will be known. And again, will be traced back to your real identity. So far we're anonymous because this address is not linked to anything but if you use on an anonymous way of transferring money into this wallet then this wallet will be linked to your identity. And then whenever you use this wallet all the transactions could be easily traced back to your real identity. Therefore, it's very important that you buy your bitcoins anonymously.

So, the first way of doing this is to create bitcoins yourself and to do that you're going to have to mine bitcoins. So, if you remember how Bitcoins work, we said that there are computers like Miners and Blockchain

Miners:

- Track every transaction
- Have a copy of the blockchain
- Blockchain:
- Public ledger
- Record of all transactions

4 ways to Buy Bitcoin Anonymously

1. Mine it by yourself
2. Exchange + Tumbler/Mixer
3. Bitcoin A.T. M Map
4. Peer-to-peer (with cash)

1. Mine it by yourself

By using their computation power to keep the blockchain working. They do this by solving mathematical problems and calculating hashes so that the blockchain functions Now these mathematical problems and the calculations they take a lot of computation power and a lot of electricity therefore not anyone can do this those who can solve mathematical problems They can generate bitcoins anonymously. It is more Powerful computers and cost- efficient but it is a Time saving process compare with others but it is very secure and very anonymous to use than also complex to communicate

2. Exchange + Tumbler/Mixer

The next way is to use an exchange. Now using Exchanges is not anonymous because when you use an exchange, they will ask for your bank information, and they will ask you to verify your identity. So, using an exchange is not anonymous, but we can combine using an exchange with what's known as Bitcoin Tumblers or Mixers**.** These are services that used to attempt to mask where the money is coming from. Therefore, it's a little bit complicated but exchanges work all over the world. So, if you couldn't get bitcoins any other way then you might have to use this way where you use an exchange with a tumbler or a mixer. Now if you just go on Google and look for a bitcoin Exchanges or use this link https://bitcoin.org/en/exchanges#international

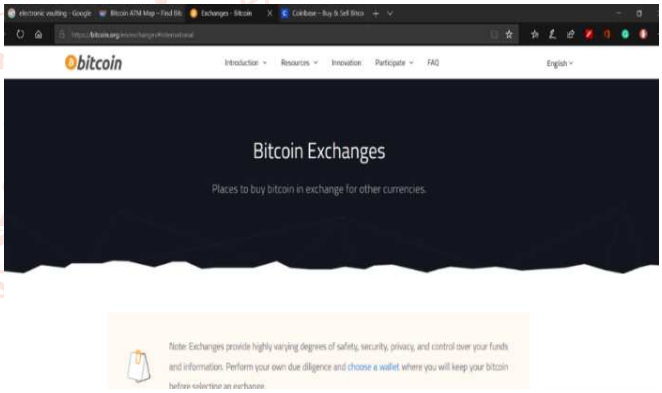

Fig.6. Bitcoin Exchanges Download page

Now on bitcoin Website itself you can see that they're recommending the following exchanges like

International level of Bitcoin Exchanges

- Bitstamp
- Coinbase
- Coinmama
- Kraken

Mixers hide source of funds. So First of all you send your coins to group of people not only for single person And then this group of people will send your money to a different wallet this way you're breaking the connection between the sender and the receiver and you can actually link a number of mixers if you want. So you can send this to mixer number one mixer number two mixer number three and then to your wallet or to someone else's wallet and you can even do this to send money to your own wallet to hide the connection that you actually own both wallets.

According to my survey, this are the more famous bitcoin Mixers
Bitcoin Laundry**:** https://bitcoin-laundry.com/
BitMix**:** https://bitmix.biz/en
http://bitmixbizymuphkc.onion
MIXTUM**:** https://mixtum.io/ - mixtum5lbuslyow2.onion

Now all of these mixers have a dark net and a clear net address so let take Bitcoin Laundry it is very cheap to use. It doesn't charge you any fees. You should only pay for transaction fees but it doesn't really do a lot of complex operations when mixing the coins, you literally send the coins and then it sends you coins back into the other wallet breaking the connection between the sender and the receiver

BitMix will work as send the coins, and they store all of the coins in one wallet. They mix the coins in that wallet, and then they give you different coins into the second wallet. But it charges a little bit more but again they're fast enough. MIXTUM is the most expensive service between the three but it is the most anonymous because when you send the coins to them, they don't simply just mix it and send it back to you. They will use this to buy Cryptocurrencies from stock exchange and then send you brand-new coins that they bought from stock exchange and from investors. Now with this the amount that you receive can also be split into a number of transactions a time delay can also be added to make it more difficult to trace these coins and link them between the sender and the receiver accounts.

3. Bitcoin A.T. M Map

Next option that we have is to use is bitcoin A.T.M. Now this is a really good option because some of these ATMs even accept cash. The only problem is not all countries have bitcoin ATMs so to check if your country has bitcoin A.T.M. you can go to A.T.M. radar .com

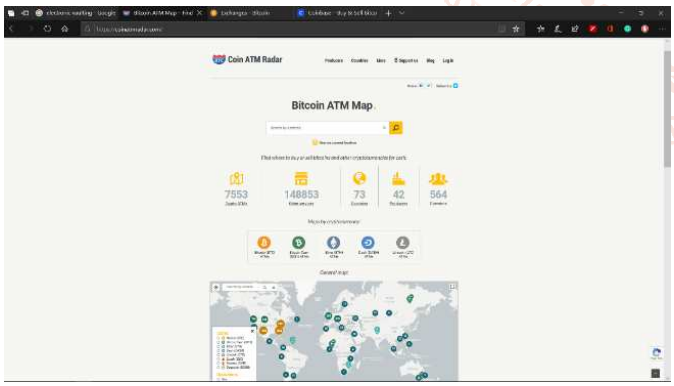

Fig.7. Bitcoin A.T.M Radar

If you're not sure if there are any A.T. M'S in your country or not you can check out this website. Coin A.T.M. radar dot com. And as you can see very easy to use all you have to do is type your country name or if you go down, you'll see a nice map that we have all of the countries in the world with the amount of A.T.M'S that they have. This map will actually show you A.T.MS for a number of Cryptocurrencies not only bitcoins. So, you can filter them from this list and here you can filter whether you want to buy or sell Cryptocurrencies or you can filter based on our location type. In show details tab you can see all details like Reviews, comments on the Bitcoin A.T. M

4. Peer-to-peer services

Next way we can use peer to peer services to buy bitcoins. In peer-to-peer services allow us to buy bitcoins directly from the seller. In this coin exchanges there is no middleman. There is no middle institution. And if the seller is willing to give us bitcoins using an anonymous method such as by giving him cash physically then this will be perfect [2].

Now you can also see that peer-to-peer services like Bisq, BitQuick, Local Bitcoins, Paxful all of these services will either require to verify your identity or they will only use services that require your identity. For example, BitQuick right here will not ask you to verify your identity but in most countries the only method of transferring money would be a method that would require your identity. Local Bitcoin used to be a really good service that would allow you to buy bitcoins in cash so you'd literally meet the person and give them cash, and they transfer the money to you. Unfortunately, recently they stopped this and you can't buy bitcoins with cash. With local bitcoin, and they also started verifying I.D. So again, this service is not very anonymous. PaxFul is a good peer to peer service that still allows you to get bitcoins by literally giving cash in person to the person that will give you the bitcoins. So it's really good

Method 2: Monero Wallet
MONERO / XMR is an open-source Cryptocurrencies and it focuses on being untraceable and private. It's similar to bitcoin It's decentralized [3]. So, there is no single entity that control it. But Bitcoin it is Private So if you analyse the whole blockchain you want to be able to get useful information on who is sending money to whom and the amount sent. So, you can see addresses but the addresses used are temporary and secured. Therefore, you can't see the actual sender and receiver and you can't see the real amount being transferred. The transactions are untraceable and the sender and receiver are not likable. All of this is confidential transactions and stealth addresses and the working is a little bit complex and it dives too much on how blockchain and Cryptocurrencies work. Tail does not have Monero software by default We have to manually install it but installation is very easy. Let's go to download page of The Official Monero Website. And download Linux based 64-bit because we are using Tails operating system. We should also check for file is modified or not so that we should also download signature and public key for verification per pass (OR) use SHA256[4] developer signature key for verification These signatures can be verified against a set of public keys without revealing the actually used private key [3].

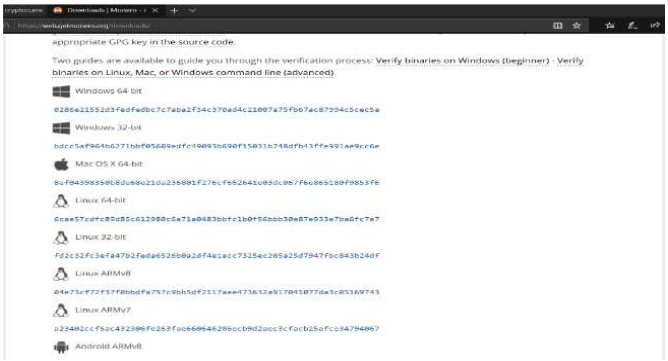

Fig.8. SHA256 developer signature according to OS

If a single bit is mismatched then don't install the file because it is modified. All the hashes are matching this

means that the file did not get modified since this hashes right.

Advantages of Monero

- Bitcoin Monero is Decentralised
- Monero is superior mining algorithm
- Monero Transactions are untraceable and unlinkable
- Bitcoin Monero is Private, it hides:
  - Sender using ring signatures.
  - Receiver using ring CT.
  - Amount using stealth address.

Installing a Monero Wallet:

Now just copy the paste the file in persistent directory and double-click it and start installing start-gui.sh is a bash file so will be executed in the terminal open the terminal in the current working directory by right clicking the directory that we want to open the terminal in and click on open in terminal. Type "ls" command and see all the files and enter "./start-gui.sh" command and the wallet graphical interface will start Installing. Change the language that you want. Next use the advanced mode because we're going to use this wallet on Tails and we'll have to manually configure it to use an online service to sync with the Monero blockchain.

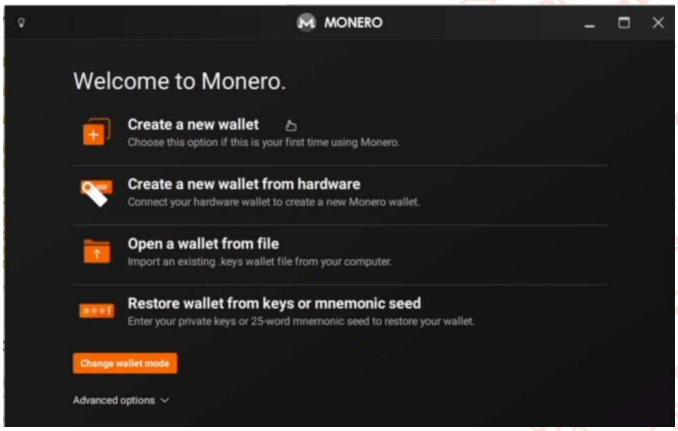

Fig.9. Welcome page to Monero Wallet

Now Create a new wallet by naming the wallet and set the wallet location. Browse the file location and save it in persistent directory [7]. Now it will show seed address copy it and paste it in a notepad it also shows block number for restoring the file click on Next and enter password and confirm password.

Next Daemon settings set as automatically in the background on your system. Total size of the Monero wallet is 25 Gigabytes so it starts extracting the file Alternatively, you can click on Connect to a remote node with this option. We're going to use a remote node to sync with the Monero blockchain. This means that we'll be able to instantly use the blockchain will be instantly able to send and receive funds, and we won't need to download the whole blockchain. So, in order to use this option, we need a remote server that will sync. Set the port number as 18099 and finish now you can see the interface of the wallet [3].

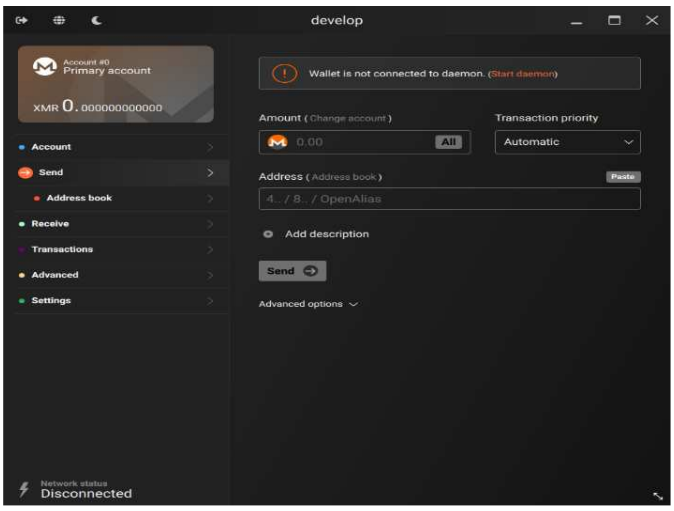

Fig.10. Account ID of Monero Wallet Crypto Exchanges

In Monero we cannot find any peer to peer services and no ATMs which you can use to get Cryptocurrencies like bitcoin. Therefore, you can get a more popular Cryptocurrencies such as Bitcoin and then exchange it to Monero [1].

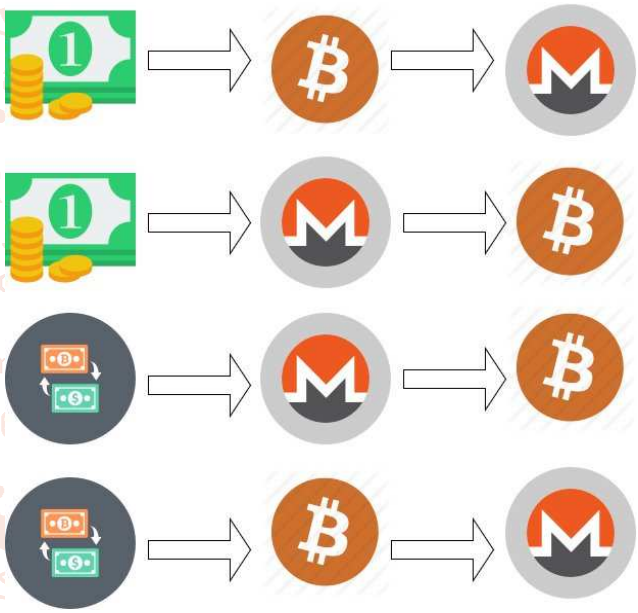

Fig.11. Cryptocurrencies Exchanges to Monero

First use cash and buy anonymous So you're already anonymous because you're using Tails operating system And then to increase your anonymity use a crypto exchange to exchange Bitcoins to Monero and then you're very anonymous and no one can trace. Alternatively let's say the end goal is you want bitcoins because you're sending money to a person or a seller that only accepts Bitcoin. What you want to be as anonymous as possible as you can buy Monero with cash again using one of the methods I explained in the bitcoin anonymous and then convert this Monero to Bitcoin using a crypto exchange. Now as you know cash is anonymous transferring the money into Monero wallet will make it even more anonymous like we said because it hides the sender and the receiver and it's not linkable and then send that to bitcoins will make your bitcoins very anonymous and very hard to trace and tie to your identity. Alternatively let's say you tried everything and you could not buy a Cryptocurrencies with cash with an anonymous then You can use an exchange service such as Coinbase and others that would verify your identity and then the money you use will be tied to your identity but you transfer that money to a

Monero wallet. Again, once you do that that link is broken because Monteiro hides the sender and the receiver using rink signatures and stealth addresses. Therefore, once you send that money to a bitcoin wallet it's very anonymous and the bitcoin address that you're going to use will not be linked to your identity even though you verified your identity when you bought the Cryptocurrencies when you bought Monero for the first time. You can do the same again use a service that verifies your identity because these are available in everywhere in the world. Now again buy bitcoins now at the last stage. The bitcoin address will be linked to your identity because bitcoin is not anonymous but once you convert that bitcoin into Monero the link is broken and this wallet right here will be very private and will not be linked to your identity. And anonymity is possible because of the way Monteiro is implemented because of the way it uses risk signatures and stealth addresses.

Now to become very anonymous. There is a concept known as churning and basically whenever money arrives into Monero wallet you can transfer it between multiple Monero wallets before sending it to another wallet or before converting it to another currency or you can literally send the money to the same wallet again with Monero sender and the receiver are not linked. So, every time you send money from one address to another even if you send in it to the same wallet that increases the distance between the wallet and the source of the funds therefore making it very difficult to trace.

Conclusion

In many countries using darknet markets is illegal even if you buy legal goods or if you're paying for legal services. The reason for this is a lot of darknet markets also include illegal goods and illegal services. So, if you're using a market that offers illegal services in many countries using this market is illegal even if you're buying legal goods. And the reason for that is you'll be considered that you're aiding a criminal organization or an organization that is involved in criminal activity. Now this is not the same for all countries like I said. So, you want to check with your country and you can always just use normal darknet markets that just don't offer illegal services and illegal goods. Still there are so many ways to exchange bitcoins, web applications to transfer Cryptocurrency in anonymous this survey paper is based on my knowledge.

References

[1] Daniel Genkin, Dimitrios Papadopoulos, Charalampos Papamanthou "Privacy in decentralized cryptocurrencies" https://dl.acm.org/doi/fullHtml/10.1145/3132696.

[2] Merve Can Kus Khalilov, Albert Levi "A Survey on Anonymity and Privacy in Bitcoin-Like Digital Cash Systems"https://ieeexplore.ieee.org/abstract/document/8325269.

[3] Felix Konstantin Maurer "Asurvey on approaches to anonymity in Bitcoin and other cryptocurrencies" https://dl.gi.de/bitstream/handle/20.500.12116/1110/2145.pdf?sequence=1.

[4] Evan Duffield, Kyle Hagan(evan@darkcoin.io, kyle@darkcoin.io)Darkcoin:Peer-to-Peer Crypto-Currency with Anonymous Blockchain Transactions and an Improved Proof-of-Work Systemhttps://assets.ctfassets.net/sdlntm3tthp6/235rllyzM8Emy64S0ew64O/0626b460d0b4bc45a298750326e15dfc/Dash_Whitepaper_-_Darkcoin.pdf.

[5] "The Merits of Monero: Why Monero vs Bitcoin" https://www.monero.how/why-monero-vs-bitcoin.

[6] J. Isaak and M. J. Hanna, "User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection," in Computer, vol. 51, no. 8, pp. 56-59, August 2018, doi: 10.1109/MC.2018.3191268.

[7] Zaid Sabih," The Ultimate Dark Web, Anonymity, Privacy & Security Course", https://www.udemy.com/course/the-ultimate-dark-webanonymity-privacy-security-course.

[8] Tails, "Installation of Tails the amnesic incognito live system", HTTPs://tails.boum.org/.

[9] "Bitcoin cryptocurrency network, blockchain vector illustration stock illustration" https://www.istockphoto.com/in/vector/bitcoin-cryptocurrency-network-blockchain-vector-illustration-gm903413146-249166322#/close.

[10] Colin LeMahieu "Nano: A Feeless Distributed CryptocurrencyNetwork"http://media.abnnewswire.net/media/cs/whitepaper/rpt/91948-whitepaper.pdf.

[11] https://www.ikream.com/5-best-anonymous-cryptocurrency-exchanges-without-kyc-verification-in-2020-27250.

[12] Electrumhttps://electrum.readthedocs.io/en/latest/faq.html#how-is-the-wallet-encrypted.

[13] Jong-Hyouk Lee Sangmyung University "Rise of Anonymous Cryptocurrencies: Brief Introduction" https://sci-hub.tw/10.1109/mce.2019.2923927.

[14] Rainer Böhme,Nicolas Christin,Benjamin Edelman,Tyler Moore "Bitcoin: Economics, Technology, and Governance" https://www.aeaweb.org/articles?id=10.1257/jep.29.2.213.