Are Cryptocurrencies Really Anonymous?

Cities & Guilds EPQ

Candidate Name: **Prajwal Dethekar**

Cities & Guilds Registration number:**FBP0331**

Centre Name: **Qufaro**

Centre Number: **006820**

Prajwal Dethekar
FBP0331

Abstract

Cryptocurrency is often touted in popular media as being untraceable and anonymous, but with major advancements in blockchain analysis techniques, and more and more stringent regulations being placed on trading, this may not be the case. In this essay, I have investigated different strategies of de-anonymising users, and if they can be effectively mitigated, regulations placed upon companies dealing in cryptocurrency and their impacts on anonymity, 2 different cryptocurrencies and their stances on anonymity and whether anonymity is only useful for criminals.

Table of contents

Prajwal Dethekar
FBP0331

Introduction

With the rapid rise in use of blockchain technology, cryptocurrency has grown more and more popular, with many different types of “coins” being created that can be used for transactions and trades. Most cryptocurrencies are often advertised as being secure and anonymous, with the foundation of a blockchain being theoretically unbreakable, and with all personally identifying data being abstracted, leaving only a unique key to identify a transaction and a unique signature to identify a user. However, as this technology evolves, more and more attacks are performed on coins, some of which could be used to ‘dox’[a1] a user and more regulations and laws are put in to prevent facilitation of criminal activity, which may undermine the privacy of a normal end-user in its wake. In this essay, I will discuss and analyse attacks on a cryptocurrency that may undermine the anonymity of a user and strategies that could be used to mitigate these attacks, focusing primarily on 2 coins: ‘Bitcoin’ and ‘Monero’ wherein I will evaluate the effectiveness of the techniques they use to ensure the security and anonymity of their users. I will also discuss laws and regulations, such as KYC(Know Your Customer) being enforced by governments on major cryptocurrency trading platforms and if the trade-off between privacy and national security is valid. I will finally evaluate if cryptocurrencies can be thought of as anonymous and the impact this would have on an increasingly interconnected society.

What is a blockchain?

To begin with, I shall define what a blockchain fundamentally is. A blockchain network contains a primary chain of blocks that has been consensually agreed upon to be the longest valid chain in the network. Miners expend CPU power to gain the opportunity to create the next block in the chain, usually recieving a reward for this effort.
Blocks contain pieces of data, such as transactions in the case of cryptocurrencies, or a link to a digital art piece in the case of NFTs[a2]. Transactions are always valid, using asymmetric encryption; A transaction is always signed by the private key of the sender, and the transaction is easily verified by checking the validity of the signature with the public key of the sender. This

ensures non-repudiation, as the sender cannot deny that they have sent what they have, data origin authentication, as the transaction must have been initiated by them and data integrity, as they must have verified the contents of the transaction, all before they signed it.

Blocks also have to contain their position in the chain, a timestamp for when they're mined, and crucially, a proof and a hash of the previous block to 'chain' them together and ensure blocks that are appended to the chain are immutable. Proofs are a value generated by a function called a 'proof-of-work' function that takes the hash of the previous block, and hashes it with a random number to find a hashed value with a consensually agreed amount of leading 0s behind it. For example, assume that for a (particularly weak) cryptocurrency, the difficulty is set to having at least 4 leading 0s, and assume the hash of a block is '8A6B099A'. With the number 1 hashed alongside it, you may get the hash '9034ABDC', which does not have the required amount of leading 0s. However, with the number 1023, you may get the hash '0000A34D', which has the required amount of leading 0s, and is thus acceptable. Bitcoin does the same, but on a much larger scale, with the proof for block #660000 being '933,627,500' and the hash being '0000000000000000008eddcaf078f12c69a439dde30dbb5aac3d9d94e9c18f6' [1], a 19 digit difficulty. This is done as hashing to get a certain amount of leading 0s requires a considerable amount of computing power, with a miner having to try many random numbers as proof before finding one that gives them a value they desire, while verifying a proof takes a significantly smaller amount of computing power.

One could create a blockchain by fitting the entirety of the previous block in the block to be created next, but this would lead to a few problems: (1) The space needed to store a block would exponentially increase, as a new block contains all the blocks before it within itself. (2) Most proof-of-work functions use the hash of the block to be able to create difficulty in terms of leading 0s. If the hash weren't to be kept within the block, a whole new method of proof-of-work would have to be derived, which would be inefficient and potentially cryptographically insecure, allowing for previous blocks to become mutable. This is why the hashes of blocks are used instead, as a hashing algorithm produces a fixed size value that is extremely susceptible to any changes in the block, so that if an attacker were to modify a block, its hash would change, which would cause the block after it to contain an invalid hash, and an attacker would have to modify and recompute the proof of each block

in the chain created after the block he modified, the difficulty of which is “analogous to a Gambler’s Ruin problem”[2], as an attacker would certainly have less computing power than tens of thousands of decentralised computers achieving the same goal, and as such, the probability of him catching up to his deficit in blocks would eventually tend to 0.
Another consensus mechanism being used in newer cryptocurrencies is called proof-of-stake. Proof-of-stake differs from proof-of-work in that coins are ‘staked’[a3] by a user to a node that is trusted communally, and that node is thus allocated a percent of mining power that they can use to determine the proof of the block. The more percent of total coins in circulation that are held by and staked to a given node, the more mining power they are given to mine a block and thus the higher the probability that they are the node to validate and mine the next block. Newer cryptocurrencies are adopting this method to “reduce the scalability and environmental sustainability concerns surrounding the proof-of-work (PoW) protocol.”[3], as proof-of-work will continually grow and use more electricity as more computers are added to a mining network, while proof-of-stake only allocates already existing mining power.
With these principles, the foundation of blockchain itself can be thought of as secure and unfailable.

Attack strategies against anonymity and mitigation

While there are many attacks that can be performed against a blockchain, most of them are unfeasible to perform, and not all of them affect the anonymity of a user. Here, I shall talk about 3 attack vectors that have been known to be used to de-anonymise users on the Bitcoin network.

1) Public IP addresses on the blockchain

Oftentimes, users of a cryptocurrency do not use proxies or Virtual Private Networks(VPNs) when connecting to the blockchain to perform transactions. This makes their public IP known to any other node they send messages to, where sending messages is necessary for performing transactions. If an attacker were to have a modified client that could store the IP address of a user who performed a transaction alongside the transaction itself, the IP address could then easily be correlated to a broad geographical position, or worse, figures of power, such as government agents or malicious actors could ask/steal from the provider of the IP address, an ISP,

personally identifying details about the user themselves, such as their full name, address and card details.
In 2018, a research article[4] was published upon a study performed by 2 professors and 2 students at Eötvös Loránd University, where upon a 2 month period, Bitcoin users were monitored using 140 modified clients distributed around the network and in different parts of the world, to ensure that as many clients as possible would connect to them. In the end, they were successfully able to identify 1,797 IP addresses belonging to unique Bitcoin addresses, which showed that it was very much possible for an adversary to monitor a network and decipher the IP addresses of particular cryptocurrency addresses en masse.
However, the study also stated that there were “three outstanding IP addresses to which 20680 users are assigned”, presuming that “These IP addresses probably belong to Bitcoin wallet services”, showing that as a potential mitigation strategy, a user could use services that would obfuscate their bitcoin address by associating the IP address to thousands of other bitcoin addresses, making it impossible to link together an IP and Bitcoin address. This however, puts all the trust into the service provider, who may or may not log one’s IP address alongside their Bitcoin address, a risk the user would have to take. Of course, simply using a VPN, a proxy, or a TOR[a4] relay would provide obfuscation too, provided that the VPN/Proxy provider, or the exit node of the TOR relay is secure.

2) Address reuse

Address reuse attacks are growing less and less prevalent as people move to more secure software wallets. The attack relies on the premise that a user uses one bitcoin address for all the transactions they perform. While this may not appear as an immediate problem, over time, a relationship graph can be drawn using all the inputs to a given Bitcoin address to determine how much bitcoin one has received, and if they were to perform a transaction with that address to an currency exchange that requires identifying information such as mail addresses or phone numbers, they could easily be identified.
This has been used for good by malware researchers, such as in 2017 by Matt Suiche, Founder of Cybersecurity Startup ComaeTech to find 3 unique bitcoin addresses in the malware code[8] to determine how much total ransom was paid to WannaCry malware controllers(49.60319339 BTC on May 24th, 2017, totalling to around £1.5 million today), and also by Assistant Professor in Electrical and Computer engineering at NYU, Danny Huang in a talk about

tracking ransomware from End-to-end[10], determining the total ransom paid and potential choke points where the ransom payments could be held, such as in exchanges where the ransomers attempt to convert the crypto currency into fiat[a5] currency to prevent them from being able to withdraw their stolen goods and potentially even find bank addresses belonging to them.
However, some anonymity can still be maintained by simply not reusing addresses, as there is no limit, and no downside to creating several hundreds or thousands bitcoin addresses to store your coins in a decentralised manner. To even prevent tracing, the coins can be transferred to the addresses using special transactions such as CoinJoin, a method that combines multiple transactions together into a single transaction that make it difficult to determine if the coins in a given address originated from a specific sender. For example[6][11], assume a simple CoinJoin Transaction, where Alice sends 2 BTC to an address she owns and Bob sends 3 BTC to an address he owns.

```
2 btc --> 3 btc
3 btc     2 btc
```

One can immediately tell that on the right, Alice is the transaction with 2 BTC, and Bob is the transaction with 3 BTC. However, assume a better structured CoinJoin transaction, where Alice again sends 2 BTC to an address she owns, but Bob sends 3 BTC to 2 addresses he owns.

```
2 btc --> 2 btc
3 btc     2 btc
          1 btc
```

This time, it is unknown which address on the left is Alice, as there are 2 possible addresses she could be. This means that Alice and Bob’s transactions are now harder to identify, being mixed together. Do keep in mind however, we can be certain that the address the 1 BTC is sent to is Bob’s, as his total BTC count must add to 3. The real benefit of CoinJoin comes with doing multiple CoinJoin transactions to end up with a scenario where it is unknown where the coins of a unique party have ended up. While this allows for anonymised transactions, this does mean one would need to cooperate with a party completely unrelated to them, for which services do exist, such as Wasabi Wallet, and JoinMarket which again, may leave identifying details such as IP addresses in the hands of third-party companies.

3) Timing/Amount correlation

Timing/Amount correlation is a simple attack that takes note of correlation between times a user says they have performed a transaction and the transaction appearing in the blockchain. It involves knowing when a person has performed a transaction and/or knowing the amount of the transaction. This attack can be performed on Bitcoin easily as the transaction ledger is completely public, meaning that anybody can see when a transaction is performed, by which and to which bitcoin address it is sent, and the amount that is sent. If Alice sent 1.134543 bitcoin at 7:00pm yesterday to bob, and Eve finds out either that Alice sent 1.134543 bitcoin, and/or that the transaction occurred at 7:00pm yesterday, or even just approximate values, she can peruse the public ledger to find out which address performed the transaction. This attack is even more potent if combined with the negligence of address reuse, as that very address can then be correlated with any other transactions which have been done using the same address, forming a financial history of Alice without her knowledge.

This was used to great effect in the talk by Danny Huang[10], whereupon using timing correlation comparing the spikes in searches on popular search engines for the ransomware and payments sent into the bitcoin addresses of the ransomware, they were able to determine if they had discovered all clusters of addresses belonging to a ransomware group, where if a spike in searches was noted while no payments were sent into the known ransomware addresses, there must still have been addresses that remained undiscovered, prompting them to expend more effort in hunting for such addresses via alternate means.

For large scale operations, such as ransomware, this is not as easy to hide, but for individuals, it is as simple as following basic internet OPSEC[a10]; hiding information that may reveal when one has performed a transaction involving cryptocurrencies, such as receipts of crypto transactions or creating social media posts on crypto transactions. If attacks do not initially know when, or how much a transaction of a given user was performed for, they do not have any information to correlate, and thus cannot succeed.

Prajwal Dethekar
FBP0331

Governmental laws and regulations on cryptocurrencies

In most countries, cryptocurrencies are heavily regulated on the grounds of preventing money laundering and combating the financing of terrorism, acronymed by AML/CFT(Anti Money Laundering/Combating the financing of terrorism). In 2018, in a hearing[12] before the US House Committee on Financial Services, Mr Yaya J. Fanusie testified that “There are enough case studies of jihadist groups experimenting with cryptocurrencies to suggest that law enforcement and the intelligence community must prepare for terrorists to try to exploit digital tokens as the technology spreads.” Centralised cryptocurrencies have been classified as financial institutions by most countries, and to be able to trade in countries that classify them as such, major centralised cryptocurrency exchanges, such as Binance, and Coinbase must conform to the regulations created by AML/CFT, implementing Know Your Customer (KYC) checks, or risk being fined, such as in the case of BitMEX, fined $100 million for violating Anti Money Laundering regulation[13]. KYC checks at the bare minimum require a user to identify themselves using an official document such as a passport or a driver’s licence to identify themselves, alongside a photo of them. More stringent KYC may also ask for their residential address and a date of birth, and even utility bills as proof of residence[14], which must all be stored alongside their cryptocurrency addresses, permanently tying them to it. While all companies that handle data must protect it under the Data Protection Act and GDPR, if the company were to mishandle the data, or even if the government wanted access to it, your anonymity would be lost. One may argue that the very storage of personally identifying information related to public keys is a complete loss of privacy, as data, no matter how securely kept, is always vulnerable to breaches.

These laws and regulations, while intruding upon privacy, are quite necessary to prevent misuse of power by large institutions to smuggle money to fund illicit activities, as financial analysis is crucial to law enforcement in understanding the motives, methods and complexity of criminal groups and is key in apprehending and dismantling felonius organisations. However, giving such access to personal data to large organisations leaves ample room for abuse; How do we know that the government won’t use this access to find journalists they disagree with, that get funded through donations to an address hosted on an exchange? Or if the financial information of a user is sold as advertising data to internet advertisers who will

then target customers in unexpected ways? Users must be aware of the ways in which data about them can be used or abused, and both governments and exchanges alike must be held morally responsible for how KYC checks affect the people.
However, there still exist ways, both legal and illegal, to circumvent such checks, such as over-the-counter(OTC) [a6] crypto trading and decentralised exchanges. Legal OTC trading does require KYC to be adhered to to operate, but OTC services regularly operate within the deep web and the dark web, offering one cryptocurrency to be traded for others, fiat currencies to be traded for cryptocurrencies, or even vice versa. Such services, while preserving anonymity, may be unreliable, as they rely heavily on built-upon trust to do most transactions and are almost certainly operating illegally, which could associate an innocent user who simply wanted a fast way to convert their cryptocurrency with cash with criminal activity, potentially incriminating them in crimes committed using bitcoin they sold to the marketplace.
Another way a user could bypass KYC is by using a decentralised exchange (DEX), such as Uniswap, to trade their pre-existing cryptocurrency for other cryptocurrency. As there is no central figure behind a decentralised exchange, they do not classify as financial institutions under the laws of most countries. This however, only allows for swappage between cryptocurrencies and not between fiat, which means a person would have to either use OTC trades to begin to trade anonymously, mine coins themselves or have coins on a personal crypto wallet stored away, potentially bought from exchanges before KYC was enforced. These methods, while not as reliable as centralised figures, embody the foundational idea of blockchain networks; to be a decentralised network that relies upon cryptographic security and not a single figure or entity to provide trust in it.

Bitcoin and its anonymity

Bitcoin is the first, and currently most popular cryptocurrency in the market. However, simply because it’s a pioneer does not make it perfect. Even in its in infancy, people were wary of calling it anonymous, opting to call it pseudonymous, as written on bitcoin.stackexchange by the Founder of now defunct cryptocurrency blog codinginmysleep.com, David Perry, who said “think of it as being an email address and then consider how your actions with that bitcoin address can be tied to you.”[19] This is due to the very

public nature of transactions on the bitcoin network, as all transactions are collated on a ledger that can be analysed, and companies for this very purpose already exist, such as Chainalysis and Elliptic. To this very day, this statement is upheld by economic experts, such as Aidan Arasasingham and Gerard DiPippo from the Center for Strategic and International Studies, who state that “Bitcoin and many other crypto assets are pseudonymous, not anonymous, meaning that their transactions and wallets can be traced.”[21]

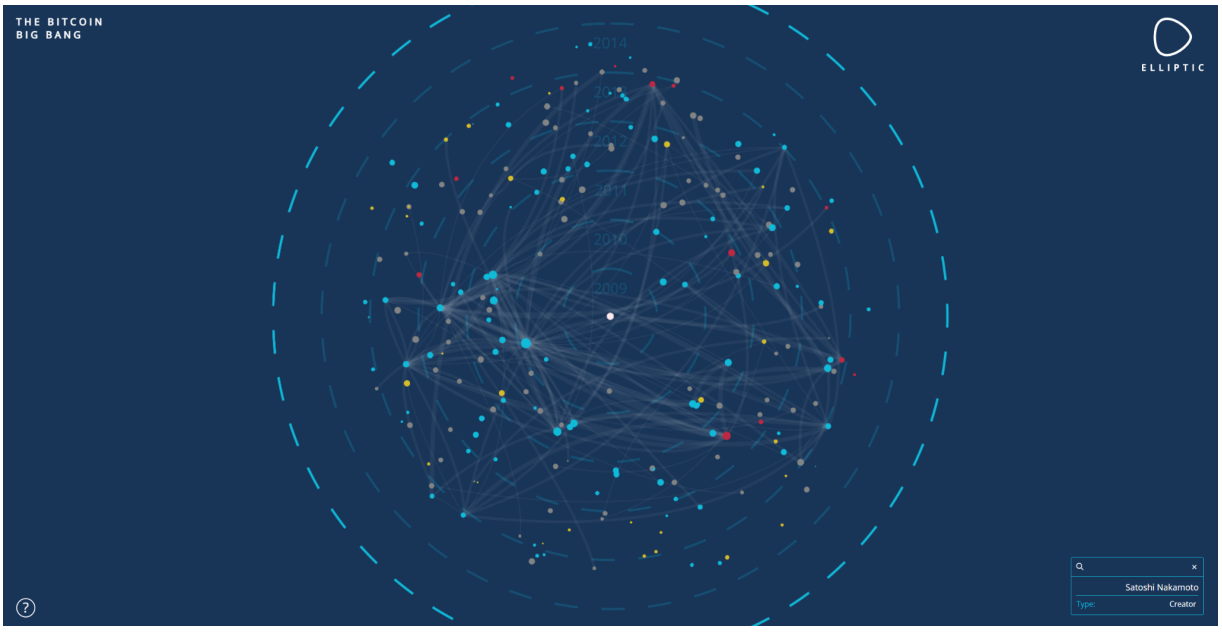
However, pseudonymity, if performed correctly, can achieve the same goals as anonymity. Indeed, the very creator of bitcoin, Satoshi Nakamoto, hides behind a pseudonym, while his real identity remains anonymous. David Perry, in the same post on stackexchange, states that “It's difficult but possible to make truly anonymous bitcoin transactions.”[19] In an incredibly insightful paper[22] by Nasser Alsalami and Bingsheng Zhan from Lancaster University, it is written that “Attacks on Pseudonymous Addressing... can be classified into two broad categories: 1) clustering and Bitcoin blockchain analysis and 2) exploitation of the Bitcoin P2P network”, and while the stance of the paper is that pseudonymous addressing is “weak anonymity”, they note that if a user were to be careful enough to use technologies such as CoinJoin to “contribute inputs in the same transaction”, they could defeat blockchain analysis. However, they note that users “rarely do so” as it adds to the complexity of creating transactions. Likewise, exploitation of the bitcoin P2P network, that broadcasts the IP address of any user making a transaction, can be defeated by using VPN services one does not need to provide personal details to, such as Mullvad, which would allow for anonymous usage of the bitcoin network. Tor has also been touted as an option, however, there exist privacy concerns over exit nodes being controlled by attackers who could monitor the real public IP address of users passing through it.

There also exist ways to “launder” bitcoins, such as sending them through services called “tumblers” or “mixers”, like Blender.io, ChipMixer and FoxMixer. These services receive bitcoin from a service user’s address, combine them with a pool of bitcoin, and then send them out to other bitcoin addresses which they then give back to the user. This means that even if the initial address’s identity is compromised, the coins are difficult to trace to their now unique addresses. Although, analysis such as amount correlation may also be used to derive the new location of the coins, most bitcoin mixers take a random fee between 1% and 5%, and most also

utilise CoinJoin and such, which increases the difficulty of such operations to be nigh impossible.

Monero and its anonymity

Monero, on the other hand, is a far newer cryptocurrency, and takes a completely different approach to privacy, selling itself as an Altcoin focused on privacy and anonymity. In the online book[23] “Mastering Monero” authored by SerHack, a security researcher and contributor to the Monero project, he states that “The only guaranteed way to exercise {one’s} right to financial privacy is to avoid revealing personal information in the first place!”. The book recognises that “a significant amount of {one’s} sensitive personal information can be exposed if {their} pseudo-anonymous blockchain identity is linked to {their} real-life identity” and that companies such as Elliptic already exist “to track and deanonymize transparent blockchains”.



The Bitcoin Big Bang, showing the spread of transactions starting from the first ever block mined by Satoshi Nakamoto.

As a solution to these privacy issues, they propose Monero, “a network that allows parties to interact without revealing the sender, recipient, or transaction amounts” in a transaction. This was achieved by using transactional proof methods such as “Bulletproofs”, a type of Zero-Knowledge proof[a7] that proves that a committed value is in a range of values, without revealing the

value itself. This allows for confidential transactions, in that the amount transferred in a transaction is not revealed, but in case a transaction has to be verified, using some very tricky math(described in [24]), it can be confirmed that a value is within a certain range.
Monero also uses a technology called RingCT, which acts as a cryptographic signature method, that allows one person to sign a transaction on behalf of an entire group, meaning that an observer cannot know for sure which one of the transactions were made by any of the users. All that is confirmed is that for one transaction, one of the users within the 'ring' of signers must have sent the transaction.
These special cryptographic techniques allow for a transaction to be validated without knowing any of its characteristics, leading to blockchains that can be defined as having "set anonymity" where "the identity of a user is either 1 out of n[a8] possible identities"[22], n being a number that can be obscenely large(must be a positive integer), making it unrealistic to decipher the identity of a user.
The entire ledger of Monero, while available publically, is indecipherable except to those who want to prove they have performed a given transaction. This reduces the possibility of blockchain analysis to a negligible amount, meaning that attacks on the Bitcoin network that rely upon recognising patterns in transactions by a user are completely mitigated on the Monero network, and the only attacks that can now be performed are exploitation of P2P networks, the effectiveness of which is again crippled, as even if the public key of a user is known and associated with their real life identity, their transactions cannot be ascertained, and thus their financial records on the Monero network are kept private. This means that many scenarios where having visible financial history on Bitcoin are now avoided, such as Price manipulation, where a seller who knew your balance could charge you more for a product, or Discrimination, where someone could see that you had spent money on a cause they did not support, and treat you unfairly.

Impacts of anonymity

Privacy is a key section in the Bitcoin whitepaper[2], and one of the biggest reasons why people use cryptocurrency over regular currency, and yet, in a survey of 20 of the most popular cryptocurrencies[22], "15 out of 20, still use the most primitive level of anonymity; pseudonymity". This may be as development into

technologies that allow people to be anonymous is often highly criticised as condonement of illegal activities. Around Bitcoin's first small boom in 2013, an Op-Ed by now Assistant Professor in Political Science at the University of Illinois, E.J. Fagan asserts that "Bitcoins essentially allow criminals to make peer-to-peer cash transactions at enormous scale." and condemns Mathhew D. Green and his creation: Zerocoin[a9], opinionating that "There is by definition no reason to avoid anti-money laundering controls other than to commit a crime, and absolutely no way for Mr. Green to prevent his system from being used for horrific actions." Fagan uses a distinct appeal to emotion, stating that "More girls will be sold as sex slaves, more rhinos will be poached, and every other large-scale transnational crime that you can name is going to become a lot easier if criminals have a way to transfer very large amounts of money completely anonymously."[25] There is a very real risk of cryptocurrency being used for illcit activities, and law enforcement agencies have to work even harder with cryptocurrency being involved, as a trail of money transferred in cryptocurrency is not as susceptible to checks and automated tripwires that would go off under AML, and are very easy to lose track of by the use of cryptocurrency tumblers, which may allow criminal organisations free reign to do evil.

On the other side of the fence, however, are people who believe privacy is crucial in creating a trustworthy currency, and that progress should continue to be made to make cryptocurrencies more private. A statement by SerHack in Mastering Monero[23] asserts "illegal activity ... has plagued every currency since the idea of money was conceived thousands of years ago." and states that Monero's privacy features give it many benefits that outweigh the negatives of enabling criminal activity. These include:

1) Fungibility; Where in regular currencies, a particular note may be 'tainted' by criminal activity traced to it and not be accepted by retailers, with a private coin, a user can be certain that their payments are accepted, as all coins are of the same value.

2) Protection against corruption/financial surveillance; In a regular bank, figures of authority, bank employees or even hackers can observe the financial history of an individual, even if not legally allowed to do so, as all data is centralised within the organisation. This allows for blackmail attempts and selling/doxxing of personal information. Using a private coin makes this unfeasible without the private key of the person involved, which is the person's responsibility, not the cryptocurrencies, to keep secret(in the same way a person would keep a bank account number secret).

Conclusions

Given that attacks that could be performed on the blockchain network to de-anonymise a user are mitigated by a user following basic rules, such as using multiple cryptocurrency addresses, concealing one's IP by using proxies or VPNs and following basic OPSEC protocols, I find that cryptocurrencies are anonymous in that regard. However, In the words of SerHack, "All cryptocurrencies are a relatively new technology, and there is no such thing as "perfect privacy.""[23] In the future, there may be more sophisticated attacks that could potentially identify users, and as such, SerHack states, "If keeping a particular payment secret is a matter of life and death, it may be risky to use *any* cryptocurrency for that transaction."

Governmental rules and regulations, applied on major cryptocurrency exchanges are key to ensuring that it is made as difficult as possible for criminals to use such services for illicit activites. However, as long as the internet were to exist, there will always be ways to bypass such rules, such as by P2P trading instead of using exchanges as intermediaries, and policing such interactions would not only be a wasted effort due to the sheer scale, but would go against one of the very reasons cryptocurrencies are decentralised, as governments are not infallible; cryptocurrencies should rely on the cryptographic integrity of the blockchain, and not trust in a central entity or figure of authority, which is why I believe that cryptocurrencies can remain anonymous despite laws to the contrary.

Between Bitcoin and Monero, while both offer ways to remain anonymous while using them, Monero does so by design, and is significantly harder to trace due to having a ledger that operates on zero-knowledge proofs, which makes it much better in terms of privacy for its users. The biggest downside, however, is the significantly smaller value of a Monero coin(193 GBP as of 18/04/2022), compared to a Bitcoin (30,162 GBP as of 18/04/2022). On a side note, Monero is also more accessible to mine and thus contribute to, as it uses a special proof-of-work algorithm(called

RandomX) that encourages CPU mining while discouraging GPU mining, CPUs being a whole lot more widespread.

Anonymity does not innately beget crime. People may require privacy for many reasons that aren't criminal, and while the impact of crime can definitely be exacerbated with the existence of essentially anonymous money transfer, it remains the responsibility of law enforcement to find alternate solutions in identifying criminals in regards to advancements in anonymity in cryptocurrencies, preferably ones that do not intrude upon the privacy of regular users.

Appendices

[a1]: Doxxing is the act of publishing private or identifying information about a particular individual, typically with malicious intent.

[a2]: NFTs (Non fungible tokens) are digital assets that represent a real-world object uniquely, which allows the owner of the NFT to own a "receipt" of the object NOT the object itself.

[a3]: Staking is the act of pledging one's coins to a node to increase the mining power allocated to that node to be used for block verification.

[a4]: Tor is software that connects a user to a volunteer driven overlay network that encrypts and runs the data they send over thousands of relays, to make it difficult to trace the internet activity back to the original user

[a5]: Fiat currency is general government-issued currency, such as dollars or the pound

[a6]: Over the counter trading is the act of interacting directly with a business dedicated to buying and selling a cryptocurrency, rather than buying it from potentially multiple people over an exchange.

[a7]: Zero-knowledge proofs allow a party to prove to another that a given statement is true without disclosing any real information about the statement. See https://en.wikipedia.org/wiki/Zero-knowledge_proof for further information(not a source, simply a definition)

[a8]: n in mathematics and computing is a placeholder for any number

[a9]: Zerocoin is a privacy focused independant coin that aimed to initially be integrated into Bitcoin, but was rejected due to performance issues

[a10]: OPSEC is a set of rules to follow to prevent leakage of sensitive information. See https://nordvpn.com/blog/what-is-opsec/ for further information.

Bibliography

[1]: 2020: Block #66000 on Bitcoin Blockchain Explorer [Online] https://www.blockchain.com/btc/block/660000

[2]: 2008: Satoshi Nakamoto | Bitcoin.org: Bitcoin Whitepaper [Online] https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf (reupload of original paper as original taken down by copyright)

[3]: 2017: Jake Frankenfield and Erika Rasuure|Investopedia.com: Defining Proof-of-Stake [Online] https://www.investopedia.com/terms/p/proof-stake-pos.asp

[4]: 2018: Péter L. Juhász, József Stéger , Dániel Kondor, Gábor Vattay | PLOS.org: A Bayesian approach to identify Bitcoin users [Online]

https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0207000

[5]: 2020: bitcoin.it: Weaknesses of Bitcoin [Online] https://en.bitcoin.it/wiki/Weaknesses

[6]: 2022: bitcoin.it: Privacy concerns of Bitcoin [Online] https://en.bitcoin.it/wiki/Privacy

[7]: 2021: bitcoin.it: Vulnerabilities involving address reuse [Online] https://en.bitcoin.it/wiki/Address_reuse

[8]: 2017: Matt Suiche | twitter.com: Bitcoin addresses found inside WannaCry ransomware [Online] https://twitter.com/msuiche/status/863082346014224385

[9]: 2020: Keith Collins | twitter.com: Live feed of bitcoin being fed into addresses related to WannaCry [Online] https://twitter.com/actual_ransom/

[10]: 2018: Danny Yuxkin Huang | IEEE Symposium on Security and Privacy: Tracking ransomware end-to-end [Online] https://www.youtube.com/watch?v=H5bPmzsVLF8 https://www.computer.org/csdl/proceedings-article/sp/2018/435301a618/12OmNx57HSS

[11]: 2021: bitcoin.it: CoinJoin [Online] https://en.bitcoin.it/wiki/CoinJoin

[12]: 2018: Mr Yaya J. Fanusie | US House Committee on Financial Services: Survey of Terrorist Groups and Their Means of Financing [Online] https://financialservices.house.gov/events/eventsingle.aspx?EventID=401565 https://web.archive.org/web/20181222131211/https://financialservices.house.gov/uploadedfiles/hhrg-115-ba01-wstate-yfanusie-201

80907.pdf(original transcript mysteriously taken down for no apparent reason)(video with his words still up)
[13]: 2021: Commodity Futures Trading Commission: Press Release of $100 million fine put upon BitMEX for violating AML [Online] https://www.cftc.gov/PressRoom/PressReleases/8412-21
[14]: 2021: Gov.uk: Money Laundering regulations for companies [Online] https://www.gov.uk/guidance/money-laundering-regulations-your-responsibilities
[15]: 2018: legislation.gov.uk: Data Protection Act https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted
[16]: 2018: gdpr-info.eu: General Data Protection Regulation https://gdpr-info.eu
[17]: 2019: Connor Dempsey | Medium.com: How OTC crypto vendors operate https://medium.com/circle-research/how-does-crypto-otc-actually-work-e2215c4bb13
[18]: 2021: Coinbase: How decentralised exchanges operate https://www.coinbase.com/learn/crypto-basics/what-is-a-dex
[19]: 2011: David Perry's Answer | bitcoin.stackexchange: How anonymous are bitcoin transactions https://bitcoin.stackexchange.com/questions/52/how-anonymous-are-bitcoin-transactions
[20]: 2015: David Perry's Blog: Opinions and thoughts on bitcoin from before it boomed https://web.archive.org/web/20160423085606/http://codinginmysleep.com/
[21]: 2022: Aidan Arasasingham and Gerard DePippo | Center for Strategic and International Studies: Cryptocurrency's role in the Russia-Ukraine Crisis

https://www.csis.org/analysis/cryptocurrencys-role-russia-ukraine-crisis

[22]: 2019: Nasser Alsalami and Bingsheng Zhang | Lancaster University: A Systematic Study of Anonymity in Cryptocurrencies https://eprints.lancs.ac.uk/id/eprint/139412/1/main.pdf

[23]: 2018: SerHack and the Monero community | Monero Project: Mastering Monero https://masteringmonero.com/book/Mastering%20Monero%20First%20Edition%20by%20SerHack%20and%20Monero%20Community.pdf

[24]: 2017: Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille and Greg Maxwell|Stanford University, University College London and Blockstream: Bulletproofs: Short Proofs for Confidential Transactions and More https://eprint.iacr.org/2017/1066.pdf

[25]: 2013: E.J. Fagan | The Baltimore Sun: Commentary on Bitcoin and international crime https://www.baltimoresun.com/opinion/op-ed/bs-ed-bitcoin-20131125-story.html