2023

# Blockchain as a Public Ledger and Means of Exchange: Policy Considerations

Madeline J. Diab

## 1. Introduction

In 2008, Satoshi Nakamoto, the pseudonym for the unknown creator(s) of Bitcoin, wanted to create a peer-to-peer means of currency exchange. At the same time, Nakamoto published his whitepaper, or his framework, for how the electronic money system would work and what kinds of needs it would serve.[1] Nakamoto's main goal was to create a system of currency exchange that could be done in a trustworthy, easy, quick, and global manner.

Cryptocurrency operates on a system of trust, and to the pioneers of blockchain, trust equates to transparency. In order to gain trust, the founders argue, there should be reliable, non-monopolized public ledger. These ledgers provide public access to all transactions that were ever made on the blockchain.[2] Wallet addresses are composed of forty-two characters, always beginning with "0x," with the following forty characters being a mix between letters and numbers. Wallet addresses on a public ledger act as pseudonyms for the user behind the wallet.[3] This means that all of the transactions made by a single wallet address (as opposed to a single person, who may have multiple wallet address) can be traced back to that wallet. While there are some currencies and third-party programs that can provide alternatives to wallet tracing, these are not commonly used in the mainstream as of now.[4] The most mainstream way to verify transactions is through a public blockchain. It is important to understand what types of

[1] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, DECENTRALIZED BUS. REV., Oct 2008.

[2] See, e.g. ETHERSCAN, https://etherscan.io/ (last accessed Dec. 1, 2022).

[3] Wallet addresses can be created by users in under five minutes with a few simple steps. Note, however, that buying cryptocurrency from an exchange (which many argue is essentially just a bank) will require more personal information, a linked bank account or debit/credit card, and in many cases, some sort of anti-money laundering (AML) or know your customer (KYC) process to purchase cryptocurrency.

[4] For example, currencies like Monero can make it difficult to trace transactions to a single wallet: "signatures are composed with outputs from the real sender's address, alongside a number of decoy addresses known as mixins" 34

technologies the mainstream gravitates toward because it will help inform how policy should be written.[5]

Bitcoin is one of the most mainstream currencies, along with Solana, Ethereum, XRP, and others. Some coins, like USDC, an acronym for United States Dollar Copy, that are backed by fiat currency.[6] These coins are called "stable coins." Stable coins are blockchain-accessible currencies that provide representations of fiat values.[7] Because stable coins are tied to traditional currencies, and do not have some of the same traits as tokens like Bitcoin. Therefore, their use cases and policy considerations are much different and thus, stable coin policy and regulation is outside the scope of this paper.

Bitcoin transactions are financial transactions, they therefore contain personal information about the users behind the wallet address.[8] Because the transactions are made on a public ledger, personal information becomes publicly accessible. This public accessibility raises questions about whether privacy laws should cover bitcoin, and if so, where lawmakers should look when developing these laws. The ideal solution would regulate the accessibility of personal information stored on the blockchain while still allowing mainstream blockchain transactions to be trustworthy, simple, and relatively inexpensive. Governments can do this by implementing a financial institution designation for cryptocurrency exchanges that are issuing large sums of

[5] El Salvador and Central African Republic have both adopted bitcoin as an official currency of their countries. CNBC, *Central African Republic Adopts Bitcoin as Legal Tender*, https://www.cnbc.com/2022/04/28/central-african-republic-adopts-bitcoin-as-legal tender.html#:~:text=The%20Central%20African%20Republic%20has,a%20statement%20from%20the%20presidency (last accessed Nov. 18, 2022).
[6] Usman W. Chohan, *Are Stable Coins Stable?*, NOTES ON THE 21ST CENTURY (CRBi) (2019), http://dx.doi.org/10.2139/ssrn.3326823 (last accessed Nov. 18, 2022).
[7] *Id*.
[8] *See* Noah Walters, *Privacy Law Issues in Blockchains: An Analysis of PIPEDA, the GDPR, and Proposals for Compliance,* 17 CAN. J. OF L. AND TECH. 1, 25 *(2019).*

currency – they can confirm personhood of those seeking funds. In addition, governments require each user of blockchain networks to complete a blockchain-based anonymous KYC process. Blockchain can offer a successful, useful, and economically efficient way to complete payments but will only last as a mainstream concept if the government does not over-regulate. Informed consent can help create clear boundaries between governmental access to personal information and crime-deterrent checks and balances. Regulation should maintain the essential elements of blockchain, but protect users against crime and fraud. Because cryptocurrency transactions are integrated globally, the discussion about potential policy creation necessitates a universal view.

This paper considers European Union (EU) and Canadian approaches to privacy and the the different sources of law from which to derive policy law in the U.S. However, the discussion of policy should consider the way that regulations affect those globally, and especially in the global south because citizens of volatile economies have benefitted from the widespread use of cryptocurrency. Part of being a responsible global citizen means considering how our actions affect the welfare of the global economy.

This paper considers the ways that blockchain is integrated into global society and how privacy concerns surrounding the public ledger are governed to date. Further, this paper discusses the tensions between current regulations and the utility of blockchain. Lastly, this paper synthesizes the main values of cryptocurrency users with the legitimate concerns about fraud and cybercrime.

## 2. The Essence of Cryptocurrency as an Exchange of Value

Nakamoto's contribution to the world Nakamoto sought to create a decentralized system of value transfer.[9] A decentralized system is one that is not run by an elected or appointed government, but by users of the system.[10] In theory, there should not be one entity in control, but in reality there are usually a few important players. Nakamoto's bitcoin processes transactions using what he calls a "proof-of-work" system which operates on a public ledger.[11] The public ledger is available to view by anyone (regardless of whether a person has contributed to the blockchain).

Trust is the key component in Nakamoto's advocacy for bitcoin. In simple terms, the proof-of-work system functions in the following way: users donate computer processing power (the "proof" in proof-of-work) to solve a complex math problem (the "work" in proof-of-work) in order to contribute to the verification of a transaction.[12] Each of these individual computers donating the processing power is considered a "node," and at least fifty-one percent of the nodes contributing to the transaction must successfully complete the math problem in order to actually verify the transaction. Because it takes massive amounts of computer power resources to validate a transaction, it would be very difficult, painstaking, and expensive to commit a fraudulent transaction.[13] Ultimately, the proof-of-work system serves to provide verification of transactions on a public ledger.

[9] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, DECENTRALIZED BUS. REV., Oct 2008.
[10] *Id*.
[11] *Id*.
[12] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, DECENTRALIZED BUS. REV., Oct 2008.
[13] *Id*.

Nakamoto's framework, in addition to fraud prevention, also solves what he terms the "double spending problem."[14] The double spending problem occurs with traditional means of currency exchange.[15] As an example, if a person has a checking account with $5,000 in it and writes a check to her carpenter for $5,000, the money was spent once. If, while the check is on hold, or before the check has been deposited, she buys a $5,000 television using the debit card that is connected to her bank account, the money has been spent a second time. The double spend problem exists in this example because the first transaction had not been verified, and all it took was a few swipes of a pen for her to commit fraud. Nakamoto posits that the double spending problem would be impossible on blockchain ledger because it would be much too laborious and expensive to attempt the fraud in the first place and because "the only way to confirm the absence of a transaction is to be aware of all transactions."[16]

Lastly, blockchain transactions, while they do take some amount of expense and resources, are also a relatively inexpensive way to exchange value globally. A study done by Thomas Kim shows that because bitcoin is such an efficient means of exchange, there is a significant cost benefit to using bitcoin in international money transfers.[17] As compared with the foreign exchange market, bitcoin is much more efficient than banks because they have large infrastructure costs and complicated mechanisms to run brick-and-mortar branches.[18] On top of that, there is an additional barrier of having the infrastructure to manage foreign exchange transfers that is greatly reduced if not eliminated by bitcoin exchanges.[19] With bitcoin, users can

[14] *Id.*
[15] *Id.*
[16] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, DECENTRALIZED BUS. REV., Oct 2008.
[17] Thomas Kim, *On the Transaction Cost of Bitcoin*, 23 FIN. RSCH. LETTERS 300, 304 (2017).
[18] *Id.*
[19] *Id.*

transfer money across the globe in seconds while at home using a standard computer or mobile device.[20] Not only is it easy to use, but bitcoin provides a store of value in countries where the local currency is much more volatile than bitcoin is, like Venezuelan or Argentinian pesos.[21] This kind of currency exchange has allowed people whose local currency is stable help their friends and family in volatile economies to afford basic goods.[22] It is generally simple, quick, and relatively cheap to make international transactions using bitcoin but it can bring incredible economic benefits to the global south.

Cryptocurrencies have been adopted by users worldwide because of its core elements of trustworthiness and accessibility. Inherent in the trustworthiness and verifiability of blockchain transactions is the potential sacrifice of privacy, and as the system becomes more widely used, the need for regulation also grows.

## 3. Currently Available Solutions for Privacy

In order to understand the dynamics of privacy as it currently stands, it is important to know what currently exists to help users feel more protected when making cryptocurrency transactions. This paper focuses largely on bitcoin because of its more global adoption and because bitcoin was created with strong goals for cryptocurrency as discussed earlier. However, there are alternatives to the mainstream cryptocurrency uses.

For clarity, note that anonymization is separate from pseudonymization. With anonymity, a person cannot be connected to any other transaction made by that person. With pseudonymity,

[20] *Id.*

[21] *See* Andres F. Cifuentes, *Bitcoin in Troubled Economies: The Potential of Cryptocurrencies in Argentina and Venezuela*, 3 LAT. AM. L. REV. 99 (2019).

[22] *Id.*

a single wallet's transactions can be traced back to the same address without using that person's name. This point is important in discussions of privacy because, as contemplated by Walters, a person's pseudonymous transactions can be considered personal information, at least according to GDPR Recital 26.[23]

### *3.1 Privacy Coins*

Privacy coins are cryptocurrencies that still use blockchain ledger technology, but without publicly displaying exactly which wallet address, or user, actually made the transaction. Privacy coins can use different types of technologies. Privacy coins still have a verified payment system and ledger of transactions, but anonymize the addresses from which those transactions come.[24]

One of those alternatives is privacy coins. Privacy coins use the zk-SNARK form of cryptography. Zk-SNARK stands for "zero knowledge succinct non-interactive arguments of knowledge."[25] One of the more popular coins using zk-SNARK is ZeroCash. Privacy coins run on a blockchain that is is able to mix the payment scheme and verify the transactions of each party, confirm all of the required information, but does not publicly reveal that information.[26]

Another option for privacy technology is Ring Confidential Transactions (Ring CTs) technology. Ring CTs use "stealth addresses," which are essentially fake wallet addresses that can confirm a transaction made in order to confuse which address actually made the transaction. In other words, stealth addresses act as decoys to confirm transactions without revealing exactly

[23] Noah Walters, *Privacy Law Issues in Blockchains: An Analysis of PIPEDA, the GDPR, and Proposals for Compliance,* 17 CAN. J. OF L. AND TECH. 1, 25 *(2019).*

[24] Noah Walters, *Privacy Law Issues in Blockchains: An Analysis of PIPEDA, the GDPR, and Proposals for Compliance,* 17 CAN. J. OF L. AND TECH. 1, 25 *(2019).*

[25] *Id*. at 32.

[26] *Id*.

which wallet, or user, made that transaction.[27] One of the most popular privacy coins using Ring CT technology is Monero.[28]

There are a few downsides to the use of privacy coins. Because the blockchain transaction requires verification and an updated ledger, privacy coins require some sort of centralized control in order to function properly and maintain trustworthiness.[29] Centralization is antithetical to the values inherent in cryptocurrency transactions, and therefore it is unlikely that privacy coins will see widespread adoption. Again, widespread adoption is an important component in understanding blockchain transactions because the efficacy of the cryptocurrency system relies on its use. A more important downside to privacy coins is the great skepticism coming from the U.S. government. Because the transactions are anonymous rather than pseudonymous, it is difficult to trace where money is going, and this makes it easier for fraudulent activity and money laundering to occur on these networks.[30] Attempting to regulate privacy coins would likely place so many restrictions on them that utility would be lost and they would fall out of the mainstream.

### 3.2 *Mixing*

Mixing is an anonymization technique that verifies transactions, just as other cryptocurrencies do, but multiple transactions are "mixed" together.[31] Mixers are third-party services that receive inputs for a number of transactions, "mix" them in a way that is unknown to users, and spits out the receiving end of the transaction without connecting the sender to the

[27] *Id*. at 34.
[28] *Id*.
[29] *Id*. at 32.
[30] Noah Walters, *Privacy Law Issues in Blockchains: An Analysis of PIPEDA, the GDPR, and Proposals for Compliance,* 17 CAN. J. OF L. AND TECH. 1, 32 *(2019).*
[31] *Id*.

receiver in each individual transaction.[32] These services typically charge fees, create delays, and still not totally anonymous.[33] Perhaps the most difficult hurdle for mixing technology is that the U.S. government has already made its position clear on such mixing applications – that they are breeding grounds for criminal activity and money laundering.[34]

## 4. Privacy as a Commodity and the Privacy Dilemma

### 4.1 *Privacy as a Commodity*

The public ledger brings with it trust and accountability, but it also raises concerns about privacy. The system uses pseudonymous wallet addresses to maintain a publicly accessible record of transaction history, but it is possible and relatively easy to link a user's address to the person behind it using auxiliary information.[35] Techniques like change address detection, side-channel attacks, address tags, and address reuse can be used to identify a person behind a wallet address.[36] The publicly available details include sender's address, receiver's address, and transaction amounts.[37] Walters (2019) argues that the metadata involved in public blockchains

[32] *Id*. at 32-33.
[33] *Id*. at 33.
[34] *See, e.g.* U.S. DEPT. OF TREAS., *U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyberthreats*, https://home.treasury.gov/news/press-releases/jy0768 (last accessed Dec. 16, 2022); U.S. DEPT. OF TREAS., *U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash*, https://home.treasury.gov/news/press-releases/jy0916 (last accessed Dec. 16, 2022).
[35] Simin Ghesmati et. al., *User-Perceived Privacy in Blockchain*, CRYPTOLOGY EPRINT ARCHIVE 1 (2022).
[36] *Id*.
[37] *Id*.

does constitute personal information because it reveals personal financial transactions between users, and those transactions contribute to the identifiability of a person.[38]

Users value privacy. Ghesmati et al.'s research strongly supports users' desire for privacy.[39] The majority of the participants in the qualitative research of regular cryptocurrency users, said that privacy in transactions is "very important" to them.[40] Some users even specified that even though they are transacting on a public blockchain, they expect their participation in such transactions to be as private as traditional banking.[41] One of the tensions that users have with using cryptocurrency is the ability for cybercriminals to hack or steal without being caught – users want their own transactions to be private, but want to be able to uncover a hacker's identity.[42] Some users in the study had concerns about privacy when using exchanges (like Coinbase or Kraken) because those exchanges require know-your-consumer (KYC) protocols. These protocols require users to provide multiple pieces of personal identification with biometric verification, and KYC programs are used to conduct customer due diligence for "financial institutions" as required by the Financial Crimes Enforcement Network (FinCEN).[43] Users were

[38] Noah Walters, *Privacy Law Issues in Blockchains: An Analysis of PIPEDA, the GDPR, and Proposals for Compliance,* 17 CAN. J. OF L. AND TECH. 1, 8-9, 32 *(2019).*
[39] Simin Ghesmati et. al., *User-Perceived Privacy in Blockchain*, CRYPTOLOGY EPRINT ARCHIVE 1, 9 (2022).
[40] *Id.* at 3.
[41] *Id*.
[42] Simin Ghesmati et. al., *User-Perceived Privacy in Blockchain*, CRYPTOLOGY EPRINT ARCHIVE 1, 3 (2022).
[43] FIN. CRIMES ENF'T NETWORK, *Information on Complying with the Customer Due Diligence (CDD) Final Rule*, https://www.fincen.gov/resources/statutes-and-regulations/cdd-final-rule (last accessed Dec. 16, 2022)

most concerned with address reuse as an infringement on their private transactions.[44] Address reuse combined with address tagging poses a threat to privacy.[45]

Address reuse and tagging can help illustrate the privacy dilemma. Address tagging occurs when a computer program helps the programmer associate a wallet address with a real world identity.[46] Having only one point of input can lead a programmer to identifying a significant amount of users through their wallet addresses.[47] When an individual reuses that address, that person's transactions can all be linked to that person's identity. Because one of the benefits of blockchain is that it is a trustworthy and efficient way of making transactions, its proponents advocate for its widespread adoption as a payment system. As it becomes more widespread and is used for important transactions, private financial information can be discovered via the public ledger. Identification of addresses through address tagging plus address reuse can interfere with the privacy concerns of individuals.

### 4.2 *Current Privacy Issues in the United States*

#### 4.2.1 KYC and AML Protocols

FinCEN requires that financial institutions and financial services companies implement KYC and/or AML systems so that anyone who transacts using the institution is accounted for and traceable in the event of fraud or crime. As previously mentioned, more popular cryptocurrency exchanges and other crypto-based businesses choose to implement KYC and/or

[44] Simin Ghesmati et. al., *User-Perceived Privacy in Blockchain*, CRYPTOLOGY EPRINT ARCHIVE 1, 7 (2022).
[45] *Id*.
[46] Martin Harrigan and Christoph Fretter, *The Unreasonable Effectiveness of Address Clustering*, INT'L IEEE CONF. ON UBIQUITOUS INTEL. & COMPUTING, ADVANCED AND TRUSTED COMPUTING, SCALABLE COMPUTING AND COMMC'NS, CLOUD AND BIG DATA COMPUTING, INTERNET OF PEOPLE, AND SMART WORLD CONG., July 2016, at 368.
[47] *Id*.

anti-money laundering (AML) protocols.[48] KYC verification helps to screen customers who interact with financial institutions.[49] The logic is that having verified people using blockchain will help to track the natural persons who are transacting on the blockchain and interfere or prosecute cybercrimes or fraudulent activity should they arise.[50]

### 4.2.2 Fourth Amendment Right to Privacy

In addition, scholars like Longman have questioned the implications of public blockchain ledgers in the context of the fourth amendment.[51] The Fourth Amendment provides citizens with "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[52] The Fourth Amendment standard, developed through *Katz v. United Sta*tes, is violated when a government searches, without a warrant, for information for which a person has a "reasonable expectation of privacy."[53] Courts have grappled with whether the Fourth Amendment is implicated in a scenario where third-parties store financial information – on one hand, the person willingly gives that information to a third party, but on the other hand, financial information is sensitive and personal.[54] In more recent times, courts and Congress both began to place more emphasis on privacy.[55] Congress passed the Right to Financial Privacy Act of 1978 which further affirmed that financial information should be treated

[48] Diksha Malhotra et al., *How Blockchain Can Automate KYC: Systematic Review*, 122 WIRELESS PERSONAL COMMC'NS 1989, 1994 (2021).
[49] *Id*.
[50] *Id*.
[51] Ashley N. Longman, *The Future of Blockchain: As Technology Spreads, It May Warrant More Privacy Protection for Information Stored with Blockchain*, 23 N.C. BANKING INST. 111, 113 (2019).
[52] U.S. Const.
[53] *Katz v. United States*, 389 U.S. 347 (1967).
[54] Ashley N. Longman, *The Future of Blockchain: As Technology Spreads, It May Warrant More Privacy Protection for Information Stored with Blockchain*, 23 N.C. BANKING INST. 111, 115 (2019).
[55] *Id.* at 114-15.

as private.[56] However, even though Congress has expressed that financial privacy is a right, financial information can still be accessed via subpoena.[57] In the context of the Fourth Amendment, it will be difficult to determine how crime interacts with personal finances.[58]

### 4.2.3 Taxation and the IRS

Government overreach into the financial affairs of cryptocurrency users has also manifested through the IRS.[59] Users and buyers of cryptocurrency often worry about the tax implications of buying and selling cryptocurrency and digital assets.[60] Users worry about paying tax on their transactions,[61] but most users of crypto assets do not fully understand how taxation actually applies to their investments.[62] The IRS itself is unclear on what sort of tax treatment different digital assets should receive.[63] Obviously, nobody enjoys paying taxes, but users and investors in cryptocurrency are worried about the IRS requesting tax payments for crypto assets. In 2016, the IRS sought and received authorization from the Northern District of California for a John Doe Summons, a "summons that does not identify the person" on whom it is being

[56] *Id.* at 115.
[57] *Id.*
[58] Recently, the executives behind the FTX cryptocurrency were alleged to have committed various securities and financial crimes. Consumers whose bank accounts have interacted with FTX claim to have had their bank accounts emptied. Cole (@cole0x), Twitter (Dec. 15, 2022, 2:07PM), https://twitter.com/cole0x/status/1603466750443470848?s=12. This raises new questions about what constitutes the reasonable expectation of privacy mentioned in *Katz v. United States*, 389 U.S. 347 (1967).
[59] Austin Elliott, *Collection of Cryptocurrency Customer-Information: Tax Enforcement Mechanism or Invasion of Privacy*, 16 DUKE L. & TECH. REV. 1 (2017).
[60] Simin Ghesmati et. al., *User-Perceived Privacy in Blockchain*, CRYPTOLOGY EPRINT ARCHIVE 1, 4 (2022).
[61] Simin Ghesmati et. al., *User-Perceived Privacy in Blockchain*, CRYPTOLOGY EPRINT ARCHIVE 1, 4 (2022).
[62] Nizan Packin Geslevich, and Sean Stein Smith, *ESG, Crypto, And What Does The IRS Got To Do With It?* ST. J. OF BLOCKCHAIN L. & POL'Y: forthcoming 2023 at 22, 22.
[63] *See Id.* at 28.

served.[64] While the summons was categorized as a John Doe Summons, the effect of the summons was that the IRS forced Coinbase to provide the identification of any taxpayer who used the exchange between 2013 and 2015.[65] Because the IRS does not need to show probable cause in order to have a summons issued,[66] an IRS-backed tax issue has an even lower bar to infringe on a person's financial privacy than in a criminal Fourth Amendment issue.

Coinbase is one of the most popular and trustworthy exchanges – it is registered with FinCEN, follows appropriate KYC and AML protocols, and is subject to the Financial Privacy Act of 1978 (because it qualifies as a financial institution).[67] This means that government entities cannot access financial information from an individual through the financial institution unless the records are "reasonably described" and the individual has approved the disclosure.[68] Under this understanding, the IRS' actions in 2016 were raises an issue about what level of privacy blockchain financial transactions should be afforded.

## 5. Notable Regulations

Privacy as a commodity for consumers has been steadily growing, especially since the internet became more mainstream. Despite its steady growth, privacy law is somewhat piecemeal, or at least it has been up until this point. Even further, because the adoption of cryptocurrency as a payment system exploded so rapidly, the policy that regulates these

[64] Austin Elliott, *Collection of Cryptocurrency Customer-Information: Tax Enforcement Mechanism or Invasion of Privacy*, 16 DUKE L. & TECH. REV. 1, 11 (2017).
[65] *Id.*
[66] *Id.* at 13.
[67] COINBASE, *Help*, https://help.coinbase.com/en/coinbase/privacy-and-security/other/coinbase-regulatory-compliance (last accessed Dec. 16, 2022); Austin Elliott, *Collection of Cryptocurrency Customer-Information: Tax Enforcement Mechanism or Invasion of Privacy*, 16 DUKE L. & TECH. REV. 1, 14 (2017).
[68] Right to Financial Privacy Act of 1978 § 1102, 12 U.S.C. § 3402.

transactions feels even more piecemeal to lawyers and participants in the industry. Legal scholars contemplate the different sources of law. In the EU, blockchain transactions might already be governed by the GDPR, which covers a broad range of engagements over the internet.[69]

In Canada, it is likely that the Canadian Personal Information Protection and Electronic Documents Act governs crypto-centred privacy concerns.[70] In the United States, where there is generally a stronger emphasis on federalism, there are a few states that have deemed themselves "crypto-friendly," and some of those states are surprising, like Wyoming and Tennessee,[71] and other states consider themselves "privacy-friendly" like California and Virginia.[72] Many sources of cryptocurrency or other digital assets could have different classifications in the financial world such as securities, financial institutions, corporations with or without shareholders, and probably more. These classifications make it unclear which federal and state laws apply because such entities might not fit squarely into definitions of a financial institution, or a security, or a bank. Some of the more popular cryptocurrency exchanges have deemed themselves financial institutions under FinCEN.[73]

### 5.1 The European Union

[69] *See* Noah Walters, *Privacy Law Issues in Blockchains: An Analysis of PIPEDA, the GDPR, and Proposals for Compliance,* 17 CAN. J. OF L. AND TECH. 1, 24 *(2019).*

[70] *See Id.* at 9.

[71] Scott Cohn, *These 10 States are Leading America In Creating a Crypto Economy*, CNBC, https://www.cnbc.com/2022/07/18/these-are-the-10-states-leading-americas-crypto-industry.html (Jul. 18, 2022).

[72] NCSL, *State Laws Related to Digital Privacy*, https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx#:~:text=Five%20states%E2%80%94California%2C%20Colorado%2C,of%20personal%20information%2C%20among%20others (Jun. 7, 2022).

[73] See, e.g. COINBASE, *Legal*, https://www.coinbase.com/legal/licenses (last accessed Dec. 15, 2022); KRAKEN, *Is Kraken Licensed or Regulated?* https://support.kraken.com/hc/en-us/articles/360031282351-Is-Kraken-licensed-or-regulated- (last accessed Dec. 15, 2022).

The EU's main privacy legislation is called the General Data Protection Regulation (GDPR).[74] Some of the main protections granted by the GDPR are the right to access what data is being used and the right to be forgotten (i.e. have one's personal data deleted from collection).[75] In a public ledger, making a bitcoin transaction (without the use of any third-party mixers) is a pseudonymous financial transaction, which, under Recital 26 of the GDPR is considered to be "information on an identifiable person."[76] It is considered personal information because, if the use of additional information is likely to be used in connection with the pseudonymized information, the natural person behind the pseudonym can be identified.[77] This means that bitcoin transactions in their simplest (and most mainstream) form are governed by the GDPR.

The GDPR identifies the concept of a "controller," the company who controls the data.[78] In an instance where an entity hires a third party to process any information, payments, or other processes for the main entity, the main entity is a controller and the third party may or may not be a processor depending on its role in the processing.[79] The EU's classification raises the issue of, in a decentralized, distributed ledger, who the controller is. In a distributed ledger system, all participants are contributors to the network – is every single person who has ever transacted on a single blockchain considered a controller? Some entities use more computing power to

[74] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016.
[75] *Id.*
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] INFO. COMM'RS OFF., *What are 'Controllers' and 'Processors'?* https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/what-are-controllers-and-processors/#:~:text=The%20UK%20GDPR%20defines%20a,the%20processing%20of%20personal%20data (last accessed Dec. 15, 2022).

contribute to the blockchain – should one or many of them be considered controllers? Or, is there no controller as it is defined in the GDPR as of now? The GDPR is a gold standard of privacy protection, and it can serve as an example of a strong policy framework to legislators and policy makers. If data protection is the responsibility of the controllers, either in the EU or the American equivalent, it is unclear who the controller is on the blockchain.

The EU parliament published a research paper in 2019 which included regulatory guidance on governing blockchain transactions.[80] The paper provides a detailed analysis of all of the many interacting facets of  blockchain and how they are in tension with privacy.[81] In this analysis, the EU Parliament acknowledged how it is difficult, if not impossible to determine who the controller is in a decentralized system.[82] While the paper did not properly address how to treat already-existing blockchains, it did address the fact that in the future, blockchains should be designed with privacy in mind – not just for compliance, but for a tool of privacy.[83] Government adoption of blockchain technology can make state processes more efficient – the EU's progressive policies will be economically beneficial on a global scale.

### 5.2 Canada

Canada's PIPEDA is even broader than the GDPR, and it is not clear whether its drafters intended to make cryptocurrency and blockchain transactions subject to the Act.[84] The definition of personal information under PIPEDA means "information about an identifiable individual."[85]

[80] European Parliamentary Research Service, Blockchain and the General Data Protection Regulation, July 2019, Exec. Summary.
[81] *See Id*.
[82] *Id*. at 101
[83] *Id*.
[84] *See* OFF. OF THE PRIV. COMM'R OF CAN., *Find the Right Organization to Contact About Your Privacy Issue*, https://www.priv.gc.ca/en/report-a-concern/leg_info_201405/
[85] Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5.

Further, information is considered personally identifiable information if it "leads to the possible identification of an individual."[86] The exchange of value (i.e. money or other currency between two people does constitute personal information, and because of the metadata stored in the blockchain's public ledgers, and IP addresses are relatively easy to find, the information contained in the transaction very clearly leads to the "possible" identification of a natural person.[87]

### 5.3 The United States

In the United States, there is no federal privacy law. Section 4 of this paper considers the various sources of law that privacy law comes from – governmental agencies like FinCEN and state equivalents, the Fourth Amendment, and the IRS. There states like California, Virginia, and others that have implemented privacy regulations on a state level. These regulations are not considered in this paper because at the moment, these regulations are scattered, being updataed, and similar enough to either the Canadian or European frameworks.

## 6. An Ideal Solution

### 6.1 Key Considerations

Before discussing a solution, it might be useful to reiterate the dilemma. As personal information becomes more of a commodity, individuals are placing more emphasis on it. At the same time, the law, including case law, policy, and legislation, is trending toward a greater emphasis on privacy. At the same time, the mainstream adoption of blockchain is becoming

[86] Noah Walters, *Privacy Law Issues in Blockchains: An Analysis of PIPEDA, the GDPR, and Proposals for Compliance,* 17 CAN. J. OF L. AND TECH. 1, 8-9 *(2019).*

[87] *See Id.*

more of a reality because of its efficiency and global nature. For most people (i.e. people not using ethically grey schemes like mixers or non-mainstream privacy coins), transacting on the blockchain means transacting on a public ledger with a public, pseudonymous record. The identification of an individual with a single transaction can reveal a whole host of other financial information about that individual and potentially private information about other individuals. Broad, blind government overreach into the financial activities of citizens can infringe upon privacy rights; however, the privacy consideration should be balanced with the threat of fraud and harm that comes along with pseudonymous and anonymous payment transactions.

As the world becomes more globalized, technology evolves to serve new purposes. Because blockchain is a solution to problems within and between nations, policy should take into consideration the utility that blockchain systems provide to its citizens and to other citizens. The various laws and guidance that exist in Canada, the EU, and the US come from different sources of law. Understandably, legislation and common law take a long time to develop, but it is difficult for good faith participants in the blockchain industry to understand how to piece together the various sources of law. The EU takes a progressive stance on blockchain, and welcomes it. The EU Parliament claims that the GDPR was written in such a way that it covers all types of technology, but it also acknowledges that the enforcement mechanism, certificates from controllers, is ineffective in the case of a distributed network.[88] The paper went on to suggest that in the future, new iterations of blockchain technology should be built with privacy in mind.[89]

### 6.2 Regulating Exchanges, Marketplaces, and Platforms and KYC

[88] European Parliamentary Research Service, Blockchain and the General Data Protection Regulation, July 2019, Exec. Summary, 101.

[89] *Id*. at 102.

### 6.2.1 Centralized Exchanges

The EU's controller concept can, however, be applied to cryptocurrency exchanges, marketplaces, and platforms like Coinbase. Coinbase is one of the few exchanges that has proven its intent to comply with applicable regulations.[90] Because of this, exchanges like Coinbase are effectively controllers of data. In the future, policy should explicitly recognize exchanges like Coinbase as financial institutions or perhaps a cryptocurrency- or blockchain-specific type of designation that maintains private financial information. This would help raise the standard for the governmental agencies like the IRS to access individuals' private financial information. Legislation that makes it more difficult for the government to access personal information is a progressive way to serve the wants and needs of citizens.

Further, a designation of exchanges as financial institutions (or another highly-regulated, highly-protected type of institution) would incorporate existing anti-fraud and anti-cybercrime frameworks. For example, if an individual wanted to make transactions from the United States using bitcoin, that person could complete a KYC or AML process with a registered and vetted institution, open a number of wallets, and use those wallets to make transactions on bitcoin. In such a system, individuals making transactions can feel more comfortable knowing that their transactions are not all traceable back to that person, and policy makers can be sure that all persons transacting on the blockchain are accounted for. This system decreases the potential for fraud, money laundering, and cybercrime while hopefully maintaining a sense of privacy for individuals. In a system where each person has been identified, perhaps the U.S. Department of the Treasury will reconsider its stance on Tornado Cash, a type of mixer that has been used to

[90] See COINBASE, *Coinbase Money Transmission and e-Money Regulatory Compliance*, https://help.coinbase.com/en/coinbase/privacy-and-security/other/coinbase-regulatory-compliance (last accessed Dec. 15, 2022).

conceal the sources behind transactions.[91] The direct legislation of cryptocurrency exchanges and marketplaces can help legislators to implement progressive solutions to privacy while maintaining checks and balances against fraudulent activity. Regulating exchanges would help lawmakers to feel comfortable with users' personal information being stored with an ascertainable entity and probably in brick-and-mortar exchanges eventually. Having trust built through a centralized exchange and extra checks and balances increase the cost of transacting on the blockchain are both antithetical to the blockchain purist's ideal system.

### 6.2.2 Blockchain-Based KYC

As an alternative, but probably a less desirable option to the U.S. government, the EU has proposed a blockchain-based method of KYC and AML processes. Currently, KYC transactions require customers to provide government-issued photo identification plus an additional form of identification like a utility bill or a tax return.[92] Typically, in blockchain, exchanges or other entities[93] will hire a third-party KYC provider, embed the software into their websites (similar to how an online retailer might embed Shopify software to process payments and manage inventory), and issue a private identifier to each confirmed person. The EU Parliament has suggested a blockchain-based form of KYC that has been recommended by numerous scholars.[94]

[91] U.S. DEP'T OF THE TREAS., *Frequently Asked Questions*, https://home.treasury.gov/policy-issues/financial-sanctions/faqs/added/2022-09-13 (last accessed Dec. 15, 2022). Tornado Cash is a type of mixer called a "tumbler" that "pools" several users' transaction at once to conceal the details of the transaction while still validating and recording those transactions. COIN CTR, *How Does Tornado Cash Work?* https://www.coincenter.org/education/advanced-topics/how-does-tornado-cash-work/ (last accessed Dec. 15, 2022).

[92] Jennifer Lowe, What is KYC? Financial Regulations to Reduce Fraud, PLAID (Nov. 2, 2022), https://plaid.com/resources/banking/what-is-kyc/.

[93] For example, NFT seller Bored Ape Yacht Club required KYC in order to be entered into its lottery to purchase certain NFT assets.

[94] *See* Diksha Malhotra et al., *How Blockchain Can Automate KYC: Systematic Review*, 122 WIRELESS PERSONAL COMMC'NS 1989 (2021).

Such a system would be developed on the blockchain, which is used for storage and confirmation of information.[95] Performing KYC protocol on a permanent blockchain would allow the confirmation of a person's identity be attached to a permanent key.[96] Each time that person needs to confirm their identity again, they can use the key as proof of their personhood.[97] This system is much more cost efficient[98] because the KYC process happens only once; currently, a person with accounts at institutions requiring identification must go through the process multiple times and with multiple KYC processors. The cost efficient system is a crucial component of blockchain because it enables mainstream adoption and is especially useful as a global tool.

Some suggest that a blockchain-based KYC system would work on a decentralized model where peers would (technologically) enforce identification of humans on the network, and monitor the network for suspicious and illegal activity.[99] A decentralized system of verification will encourage trust and fair play among those transacting on blockchain networks – a key component of Nakamoto's blockchain. However, the blockchain can sometimes look like a number of larger, more centralized players working in conjunction with individual users, and this is a happy medium between a complete decentralization and a government-operated system.

### 6.3 Informed Consent

State-level legislation is trending toward, and the EU has already established, an explicit consent model for data collection.[100] In the EU, this looks like an "opt-in," as opposed to an "opt-

[95] *Id.* at 2002.
[96] *Id.* at 2016.
[97] *Id.*
[98] *Id.*
[99] *Id.* at 2003.
[100] *See, e.g.* The California Privacy Rights Act of 2020.

out" model like California's.[101] An opt-in model can help provide users with a sense of informed consent that can be withdrawn.[102] The informed consent approach is especially important as it pertains to where personal information is being used and with whom it will be shared – users of blockchain value their privacy and are worried about government involvement.[103] If users can pick and choose how their information is being used, they are more likely to be amenable to sharing any information at all.

An opt-in model could look something like the following: before processing any information, the controller informs the user about every use of that individual's data and have that user consent to each instance. In instances like the IRS' John Doe Summons in 2016, both Coinbase, as a trusted exchange, and Coinbase's customers were surprised that the court approved of the summons. Opt-in consent provides a sense of transparency to users and allows them to fully understand when and where the government is interacting with their data. To Nakamoto and other blockchain founders, it would be ideal to have no personal or pseudonymous data shared with anyone – government or not. Realistically, financial transactions require an element of government input to discourage fraud, money laundering, and cyberattacks. Informed consent can help relieve some of the tension between privacy and a public ledger system. This relief of tension is an important aspect of maintaining the utility of blockchain networks; users want little government involvement, and if users are worried about legal troubles, blockchain will not become a mainstream technology. In order for governments

[101] See EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016; The California Privacy Rights Act of 2020.

[102] Benjamin Schellinger et al., *Yes, I do: Marrying Blockchain Applications with GDPR*, 19 E-GOV'T, 22 (2022).

[103] *See* Simin Ghesmati et. al., *User-Perceived Privacy in Blockchain*, CRYPTOLOGY EPRINT ARCHIVE 1, 9 (2022).

and citizens to avail themselves of the efficiencies of blockchain as a transaction system, state authorities should keep their distance from the metaverse.

## 7. Conclusion

As concerns about personal privacy grow, and as cryptocurrency becomes more widely adopted, governments must understand and assess how to implement policies that protect personal privacy rights but still prevent and discourage fraud and cybercrimes. Regulation should allow citizens to enjoy the benefits of a public ledger, a cheap and simple way of exchanging currency, and for many, a relatively stable system of currency. An ideal solution would make user identification available only in situations that absolutely necessitate it without over-policing users' ability to transact freely on the blockchain.

A central component of blockchain is trust. The government wants to participate in and benefit from the utility that blockchain offers to citizens and needs to be careful not to overstep. In order to do so, the government can pose regulations for the way that blockchain networks work without direct involvement. Regulating cryptocurrency exchanges will deter criminal transactions from occurring on blockchain because it requires the monitoring of actions of individual persons by exchanges and not a governmental agency. Exchanges like Coinbase have established trust in the market, and will continue to do so as long as policymakers allow for it. Alternatively, or in addition, the government can require that users of blockchain networks enroll in a blockchain-based KYC system. This measure would ensure that each user has been confirmed as a person, not a bot, and it would deter crime without making the connection between the pseudonymous addresses and the verified person. In order to establish and maintain trust, any transfer by miners, exchanges, and more centralized entities on the blockchain should ensure that when processing or collecting data, they give users the opportunity to provide informed consent and revoke that consent if and when desired.

Cryptocurrency uses a distributed ledger system in which users contribute to the verification of transactions. These transactions take a significant amount of power to confirm, and a reversal of a transaction on the blockchain network would be useless, making it unattractive for hackers and fraudsters to interfere with. The system was set up by Satoshi Nakamoto to instill trust in users. Cryptocurrency is an easy way for users to send money to friends and family abroad, and often, currencies like bitcoin are much more stable in value than some fiat currencies like the Venezuelan peso. Currencies can be accessed by a wallet that takes less than five minutes to create on any computer or mobile device. Trustworthiness and accessibility have contributed to the growth of cryptocurrency.

Blockchain transactions are made using wallet addresses as pseudonyms for the user who owns the wallet, and while a certain address' transactions can generally be traced when making simple bitcoin transactions, there are mechanisms like mixers and privacy coins that can hide the exact transactions made by a particular user while still recording that transaction on a public ledger. These extra steps toward anonymity have raised eyebrows among the U.S. government because of their potential for money laundering and cybercrime. Because of these criminal concerns, governments should seek to regulate cryptocurrency transactions in a way that allows users to feel protected but not exposed.