PRIVACY, TAX EVASION, AND THE DEVELOPMENT OF CRYPTOCURRENCIES

Philipp Ruppert*

CITE AS: 1 GEO. L. TECH. REV. 401 (2017)
https://perma.cc/6VJ7-AN6N

INTRODUCTION

In an increasingly globalized world, the emergence of decentralized systems of virtual currency has created a way for individuals to quickly and easily transfer value directly to one another without the need for a trusted third-party intermediary. While this is useful to many individuals, it creates challenges for society. Cryptocurrencies,[1] such as Bitcoin, are often anonymous, and governments lack the ability to regulate or even track transfers. This can facilitate crime, as in the case of Silk Road, an online marketplace for the illegal sale of drugs and weapons.[2] Some users have also reported theft of their virtual currencies, which is difficult to even prove as a

* GLTR Staff Member; Georgetown Law, J.D. expected 2018; KU Leuven, Ph.D. candidate; Columbia University, M.S. 2015; University of Warwick, B.S. 2013.

[1] Cryptocurrencies in this context are electronic currencies that use encrypted peer-to-peer communication in order to transfer value.

[2] *See*, Benjamin Weiser, *Man Behind Silk Road Website Is Convicted on All Counts,* N.Y. TIMES (Feb. 4, 2015), https://www.nytimes.com/2015/02/05/nyregion/man-behind-silk-road-website-is-convicted-on-all-counts.html [https://perma.cc/NS87-TW5Y].

result of their anonymous nature,[3] and there is the further potential of these currencies being used to facilitate tax evasion. Ultimately, it may be possible that the advantages of digital currencies do not have to coexist with the current disadvantages. Identifying why legal users seek anonymity in cryptocurrencies and what that anonymity provides could lead to a better application of the technology to harness its potential without increasing crime. This literature review will discuss Prof. Omri Marian's publications regarding cryptocurrencies and tax evasion, privacy in general, as well as anonymity in cryptocurrencies. It will conclude by suggesting alterations to the framework proposed by Marian that could achieve both privacy, and control over tax collection.

MARIAN'S RESEARCH AND CONCLUSIONS

Cryptocurrencies have proven challenging for governments because anonymity and lack of trusted intermediaries, such as banks, allow the currencies to be used as tax havens by their users.[4] Marian considered these challenges in his 2013 article, *Are Cryptocurrencies Super Tax Havens?*. He outlines two parallel developments that could potentially lead to cryptocurrencies becoming untraceable tax havens, namely increasing use of cryptocurrencies, and the reliance of tax enforcement on financial intermediaries.[5]

The first development is the increasing popularity and acceptance of cryptocurrencies, coupled with their anonymous and untaxed nature. Cryptocurrencies are now accepted in a range of businesses, and the most successful one, Bitcoin, is accepted even by major retailers such as Microsoft, Dell, and Subway.[6] Bitcoin's availability as a medium of exchange for goods and services eliminates the necessity for Bitcoins to be converted back to traditional currency, making it increasingly integrated in the real economy.[7] The second development is the targeting by the U.S. government of financial

---

[3] Fergal Reid & Martin Harrigan, *An Analysis of Anonymity in the Bitcoin System, in* SECURITY AND PRIVACY IN SOCIAL NETWORKS 197, 214 (Yaniv Altshuler et al. eds., 2013).
[4] Omri Marian, *Are Cryptocurrencies Super Tax Havens?*, 112 MICH. L. REV. FIRST IMPRESSIONS 38, 38-39 (2013).
[5] *Id*.
[6] *See,* Jonas Chokun, *Who Accepts Bitcoins As Payment? List of Companies, Stores, Shops,* (Feb. 6, 2017), https://99bitcoins.com/who-accepts-bitcoins-payment-companies-stores-take-bitcoins/ [https://perma.cc/9VHH-T9PZ].
[7] Marian, *supra* note 4, at 39.

intermediaries in order to combat current tax evasion. The Foreign Account Tax Compliance Act (FATCA) is aimed at punishing foreign banks for failing to disclose the identities of accountholders, when those accountholders are U.S. taxpayers.[8] Consequently, there have been a number of arrangements between the United States and other nations to circumvent foreign bank secrecy laws, and thereby expose tax evasion by U.S. citizens.[9] Taken in combination, the anonymity and lack of intermediaries in the transactions make it impossible to continue the intermediary-based tax enforcement mechanisms, and will lead to cryptocurrencies becoming tax havens for U.S. tax payers.[10]

In 2014, Marian revised his paper based on newly available research, in the article *A Conceptual Framework for the Regulation of Cryptocurrencies*.[11] In this work, he proposes a regulatory framework that would maintain the current levels of privacy and cost to criminal action despite the development of cryptocurrencies.[12] Marians's argument updates the premise of both developments outlined in his previous paper. It concedes that Bitcoin is not actually anonymous, and that its pseudo-anonymous nature leads to the possibility of tracing money transfers and potentially identifying users. Similarly, it recognizes that intermediaries are a result of market forces and have naturally developed in various forms in the Bitcoin market as well. He also identifies major retailers as a good intermediary to leverage in combating illicit activity in this new system.[13]

Marian recommends an elective tax on anonymity during a purchase.[14] In his framework, a buyer using a cryptocurrency account could either pay an anonymity tax when making a purchase or disclose his or her identity, at which point the tax would not be levied. He proposes for this cryptocurrency transaction tax to be more likely to result in an over-collection of taxes after the assumption that no income tax has been paid on the money used.[15] This would incentivize the user to identify themselves,[16] for example through a

[8] *Id*. at 41.
[9] *Id*. at 41.
[10] *Id*. at 46.
[11] Omri Marian, *A Conceptual Framework for the Regulation of Cryptocurrencies*, 82 U. CHI. L. REV. DIALOGUE 53, 53-54 (2014).
[12] *Id*.
[13] *Id*. at 66.
[14] *Id*. at 64.
[15] *Id*. at 65.
[16] Marian, *supra* note 11, at 65.

private identification number, as it already exists in credit or debit cards.[17] Finally, Marian addresses various possible criticisms of his regulatory system, including the assumption that it would break down if a completely anonymous cryptocurrency was created. He concludes this statement by suggesting that such a currency would be unlikely to succeed, considering there is a necessity for trust in the financial market.[18]

In the first part, this literature review will consider the utility of privacy and anonymity for legal users of a currency, and will give an outline of the current judicial view on the right to privacy in the context. The second part will further analyze the anonymous nature of cryptocurrencies and argue that a completely anonymous system may not only be possible, but could be successful in the market. Finally, the third part will examine the implications such an anonymous currency would have on Marian's proposed cryptocurrency transaction tax, both in the context of tax evasion and criminal activity in general.

PRIVACY AND ANONYMITY IN SOCIETY

In his 2014 paper, Marian attempted to create a framework of regulation that would allow for privacy in banking to stay approximately at the level it is now. He argued that, while privacy hindered tax collection, privacy has its own societal advantages, and maintaining the currently level of financial privacy may be desirable.[19] In order to better contextualize Marian's argument, the following section will outline a number of definitions of privacy, how privacy may serve society, and what types of privacy other than anonymity could serve the user base of cryptocurrencies.

A right to privacy in American law was first mentioned in a Harvard Law Review article by Warren and future Justice Brandeis, who defined it as a "right to be left alone."[20] Papers in sociology, psychology, and philosophy, however, have progressed beyond that definition.[21] While the advantage of embarrassing facts about an individual staying private is likely the most obvious, the use of privacy also extends to everyday life. In a 1975 article, the

[17] *Id*. at 62.
[18] *Id*. at 67.
[19] *Id*. at 56.
[20] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).
[21] Katayoun Baghai, *Privacy as a Human Right: Sociological Theory*, 46 SOC'Y. 951, 952 (2012).

philosopher James Rachels argues that the multifaceted nature of humans and their interactions makes some level of privacy necessary.[22] While someone may employ one type of behavior towards a child, the same person will show different behavior towards a co-worker, spouse, or political figure. Thus, it is important for that person to be able to select the way they are perceived by each audience, an ability which is furthered by autonomy over one's information. Privacy can therefore also be understood as a person's ability to control the information they provide to each group of people, or selective self-presentation.[23]

This concept can also be expanded to society as a whole. With various groups representing "one-tracked and monopolistic" viewpoints, individuals require the use of discretion and privacy to navigate the intricate web of social interaction and exist on a spectrum in-between.[24] In consequence, each person only knows that which is required of them to know within any given social context, be it private, public, or business-oriented. This allows for individuals to both represent themselves as they wish to in each interaction, and to minimize the difficulty of remembering information irrelevant to the context.[25] Verschraegen argues that such compartmentalization of information is also useful for government, as "prohibition of political interference in legally recognized private spheres relieves the political system from decision making on a wide range of issues."[26] In essence then, privacy serves society by allowing information to be compartmentalized to its relevant audiences, relieving others of responsibility, as well as allowing individuals to exist on a continuum between extreme attitudes.

Looking at currency in particular, it is clear that most financial transactions will transcend groups, identities, and behavior. The same person who may be donating to a Democratic campaign could be donating to pro-life organizations, using the same currency to do both. While there may not be a problem with that, it should be the choice of the individual whether to disclose either one of those actions to the other group, and a lack of privacy in financial transactions threatens the ability to do so. This issue also touches on the subject of equality. Will one of the groups behave differently towards the individual if they know about the other donation? Does the individual have a

---

[22] James Rachels, *Why Privacy is Important*, 4 PHIL. & PUB. AFF. 323, 326 (1975).
[23] Baghai, *supra* note 21, at 956.
[24] *Id*. at 954.
[25] *Id*.
[26] *Id*. at 957; G. Verschraegen, *Human Rights and Modern Society: A Sociological Analysis from the Perspective of Systems Theory*, 29 J. L. & SOC'Y. 258, 272 (2002).

right to be treated equal to everyone else in the group regardless of tangentially related activities?

However, as is often noted in similar discussions,[27] privacy rights can also shield criminality. If perpetrators will be treated equally to everyone else in other contexts, illegal actions will have less negative impact on their lives, decreasing the potential cost of such conduct. As mentioned by Marian, this will increase the utility of criminal action, leading to an increase of such behavior by rational actors.[28]

In the context of privacy as compartmentalized information, it may not be necessary to have total anonymity, however. In 1967, Westin proposed four states of privacy: Solitude, anonymity, reserve, and intimacy.[29] Solitude is defined as a removal from other people and not applicable here. Anonymity refers to the state of interacting with others without disclosure of one's identity, and is what is so far the goal of many cryptocurrency developments. Reserve describes a person's control over the disclosure of information. Finally, intimacy is the state of disclosing information only within an in-group environment.[30] The final two categories are most applicable to the description of privacy above, and were also analyzed in the context of online interaction before: In psychological literature, Taddiken investigated privacy in the context of social interaction, and came to the conclusion that forms of privacy other than anonymity can serve to achieve gratification for social media users.[31] Transferred to financial interactions, it may therefore be possible to satisfy the need for privacy needed without resorting to anonymity. Better separation of who has access to what set of information about a user's financial transactions could even lead to increased privacy as well as increased cost of criminal action.

Privacy in Law

While sociological and psychological papers show the need of both society and individuals for privacy, and suggest that it was already around before the modern systems of government, the concept of a legal right to

---

[27] Sarah Meiklejohn et al., *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*, 59, 4 COMMC'N OF THE ACM 86, 86 (2013).
[28] Marian, *supra* note 11, at 60.
[29] *See*, ALAN F. WESTIN, PRIVACY AND FREEDOM 31 (1967).
[30] Monika Taddicken & Cornelia Jers, *The Uses of Privacy Online: Trading a Loss of Privacy for Social Web Gratifications?*, PRIVACY ONLINE 143, 145-148 (2011).
[31] *Id*.

privacy is relatively young. It was only in 1890 that the right of privacy was suggested in the Warren/Brandeis article in Harvard Law Journal.[32] Consequently, there are not as many judicial decisions about the right per se as one would expect. However, it is possible to assess the judicial opinion on privacy from the opinion's balancing between the interests of individuals and the state.[33]

In the *Bowers v. Hardw*ick[34] and *Lawrence v. Texas*[35] line of cases, the Supreme Court weighed whether the Fourteenth Amendment protection of liberty and privacy extended to homosexual sodomy in the petitioners' home. Overruling Bowers in Lawrence, the Court ultimately concluded that it did, stating that petitioners were "entitled to respect for their private lives."[36] Similarly, a lot of Fourth Amendment jurisprudence weighs an individual's privacy against the government interest to pursue crime. In this regard, the Supreme Court decided in *Silverman v. United States* that even intruding into the home by a fraction of an inch would be too much,[37] and then extended this protection in *Katz v. United States* to places in which an individual had manifested a subjective expectation of privacy that was seen as reasonable by society.[38] In *Tehan v. United States*, the Court also stated that the Fifth Amendment reflected the right of an individual to have "a private enclave,"[39] and in *NAACP v. State of Alabama* stated that the First Amendment gave an individual "freedom to associate and privacy in one's association."[40] While many of these cases show that the Supreme Court strongly recognizes the right of individual citizens to live undisturbed from government interference, Fourth Amendment jurisprudence of the Court also shows a different approach when it comes to information already disclosed to third parties. In cases such as *United States v. Miller*, the Court has repeatedly held that the Fourth amendment does not protect information disclosed with third parties, even when the information has been disclosed on the assumption that it will be limited in use.[41]

---

[32] Warren & Brandeis, *supra* note 20.
[33] Baghai, *supra* note 21, at 959.
[34] Bowers v. Hardwick, 478 U.S. 186, 186 (1986).
[35] Lawrence v. Texas, 539 U.S. 558, 558 (2003).
[36] *Id*. at 578.
[37] Silverman v. United States, 365 U.S. 505, 512 (1961).
[38] Katz v. United States, 389 U.S. 347, 347 (1967).
[39] Tehan v. United States ex rel. Shott, 382 U.S. 406, 416 (1966).
[40] NAACP v. State of Alabama, 357 U.S. 449, 462 (1958).
[41] United States v. Miller, 425 U.S. 435, 445 (1976).

While these decisions of jurisprudence extend clear protection to certain aspects of an individual's privacy, they are largely in line with the "right to be left alone" explained by Warren and Brandeis. Looking at the concept of privacy as a separation of information for relevant audiences as suggested by Baghai, the current state of judicial decisions seem to be a strong violation of the individual's interest in controlling the information about themselves. If an individual discloses information to a third party, such as a bank, an insurance provider, or a telecommunication provider, such information would not be considered protected. This is the case even though the individual may have very deliberately exercised a level of control over which information they have shared with which group. It therefore seems that, while the judicial system strongly supports the right to privacy, the jurisprudence has not yet moved beyond the context of Warren. In light of increasing collections of information vital to a person's identity online, such a move may however be necessary, especially if the judicial system wants to remain true to the statement made in NAACP. Notably, Justice Sotomayor's concurrence in *United States v. Jones* pointed out that "the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties . . . is ill suited to the digital age . . ."[42]

In summary, it appears that the need for privacy of financial interactions and the government's need to control criminal activity may not be mutually exclusive. Since anonymity in financial interactions is not necessarily a requirement for privacy of an individual's actions, the move towards a separation of the two will require a recognition of the separation of various types of information by the government. While the legal system does support the right of privacy for an individual, the current perspective on privacy as a right to be left alone will not be sufficiently subtle to support such a separation.

ANONYMITY IN CRYPTOCURRENCIES

While technology seems to present further complications for privacy, making the balancing act between various interests of society and individuals increasingly difficult, technology may also provide the solution. Assuming that privacy is served through guaranteeing that only a permitted group has access to any one area of information at a time, it may be possible to technologically grant the government the ability to access an individual's

[42] United States v. Jones, 565 U.S. 400, 417 (2012).

records to detect tax evasion or criminal activity, while decreasing access to other types of information and therefore increasing the level of privacy the individual enjoys. In that way, the technology itself could move towards a compromise with the current legal system, allowing for faster adaption of the judicial decisions to the currencies. The following section will outline the current state of cryptocurrency anonymization, as well as developments towards this direction.

How Do Cryptocurrencies Work? The Example of Bitcoin.

Any electronic currency has to implement mechanisms to establish ownership, protection against double spending, anonymity, privacy, and issuance of new currency.[43] After a number of less successful electronic currencies, Bitcoin's success was based on how it addresses these challenges, which has been copied in a number of later attempts. Since there is no central authority to issue currency, Bitcoin currency can be generated by anyone through "mining." With Bitcoin, miners use special software to solve complex math problems and are issued a certain number of bitcoins in exchange.[44] Each user can make a public statement to the Bitcoin network, stating the amount of Bitcoin transferred, as well as accounts from which to transfer and accounts to transfer to. The Bitcoin network records any such transactions of existing bitcoins between users, which are added to a public ledger, called the blockchain. The process of mining does not only create new currency, but is the process of creating the next entries in this ledger, which is essential for the operation of the system. Bitcoin are kept in a "wallet," specialized software that stores the public and private key pairs associated with previous and potential transactions.[45] Every transfer between two accounts has its own public key to be identified, as well as the previous owner's private key to authorize the transaction. While it is possible to reuse a public key for a transaction, it is generally considered good practice to create a new pair of keys for each transaction. Since no identifying information is needed in the creation of a wallet, there is a certain level of initial anonymity associated with Bitcoin. The blockchain is particularly notable, as the decentralized

[43] Reid & Harrigan, *supra* note 3, at 200.

[44] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN (Mar. 27, 2013), http://bitcoin.org/bitcoin.pdf [https://perma.cc/BZG2-NHA5].

[45] Public keys can be understood as the publicly identifiable number of each transfer, a private key as the "password" to confirm ownership of the transaction. *See, e.g.* Reid & Harrigan, *supra* note 3, at 203.

nature of the system requires this public ledger as a safeguard against double spending.[46] However, the availability of the entire transfer history also means that there are many data points from which it is possible to reverse engineer information on users or user behavior.

Bitcoin Anonymity

Even though Bitcoin has been treated as a currency in which users enjoy anonymity during the first years of its operation, anonymity in cryptocurrencies is not as easily achieved as one might assume. In the past 4 years, various academic papers have looked into the anonymity aspects of cryptocurrencies in general, and Bitcoin in particular.

Bitcoin can consequently be said to not reach to the level of anonymous transactions. Various papers have used the blockchain ledger in order to passively analyze the transactions and user bases of Bitcoin, identifying up to 40% of users through various methods.[47] In particular, grouping many accounts and transactions together by using the underlying transfer rules and accepted procedures in Bitcoin, makes it possible map the system and trace money. For example, if one public key is associated with a real ID, such as a tweet of a public key to elicit donations, it is possible to also identify other public keys (and therefore bitcoins) that are likely owned by the same user, but have not been publicly mentioned. Adding to this, the analysis of TCP/IP[48] makes the system even more vulnerable to deanonymization. Koshy et al. were able to create a mapping of the network independent from blockchain analysis.[49] This was furthered by Kaminsky, who used

[46] Double spending concerns the potential problem of an existing bitcoin being sent to two different recipients without the system being able to realise this in time. See, e.g. Jordi Herrera-Joancomartí, *Research and Challenges on Bitcoin Anonymity*, *in* 8872 DATA PRIVACY MANAGEMENT, AUTONOMOUS SPONTANEOUS SECURITY, AND SECURITY ASSURANCE, LECTURE NOTES IN COMPUTER SCIENCE 3, 5 (Joaquin Garcia-Alfaro et al. eds., 2015).

[47] *Id*. at 9.

[48] TCP/IP or Transmission Control Protocol/Internet Protocol refers to the protocols underlying basic communication between computers on the internet. *See, e.g*. *Definition of: TCP/IP*, PC MAGAZINE, http://www.pcmag.com/encyclopedia/term/52614/tcp-ip (last visited Apr. 4, 2017) [https://perma.cc/B93F-PAQ9].

[49] Philip Koshy et al., *An Analysis of Anonymity in Bitcoin Using P2P Network Traffic*, *in* 8437 FINANCIAL CRYPTOGRAPHY AND DATA SECURITY 469, 467 (Nicolas Christin & Reihaneh Safavi-Naini eds., 2014).

combination of the blockchain analysis with TCP/IP in order to map user accounts to IP addresses and therefore locations.[50]

All of these possible attacks are facilitated further by active participation. Meiklejohn et al. used their bitcoins, transferring them to known users in order to trace the flow of their money through the system and deduce additional information.[51] This is very effective on the level of individual attackers, but would be even more so if it were conducted by a government that is capable of legally compelling the participation and disclosure by many legitimate actors. In particular, compelling the naturally formed intermediaries would add to the effectiveness of such an attack. While services that exchange Bitcoin with real currencies used to be the dominant intermediary, there has also been a development of online wallet providers, coin swapping services, and others which have gained prominence.[52] The online wallet providers, for example, make Bitcoin wallets more accessible to the general public by merely requiring a setup similar to an email account. Further, wallets do not require their own software and may be access from a web browser on any device. This function resembles a bank at the front end, holding the account information of various customers, but is not comparable to a traditional bank in the back-end service, as it is not holding the money or facilitating the transfer. The convenience of online wallets comes at the expense of decreased security, as service providers generally keep record of at least, but sometimes more than, one IP address associated with an account.

Overall, the anonymity in Bitcoin does not appear to be particularly strong. With an increasing number of confirmed data points, it becomes much easier to determine the identity and behavior of the others. Because the blockchain contains all transfer data, users may be easily identified, and even users that actively protect their identity may be vulnerable. It is important to note, however, that bitcoin was not created to enable complete anonymity,[53][54] and that maintaining the core script's integrity takes precedent with the community around the code. Thus, while multiple processes have been proposed for increasing the anonymity of Bitcoin, none of them have been implemented or are likely to be implemented. Consequently, there are a range of alternative cryptocurrencies that are not yet as common as bitcoin, but which are built on lessons learnt from its vulnerability to deanonymization.

---

[50] Reid & Harrigan, *supra* note 3, at 202.
[51] *See generally* Meiklejohn et al., *supra* note 27, at 89.
[52] Marian, *supra* note 11, at 53-54.
[53] Nakamoto, *supra* note 44.
[54] Reid & Harrigan, *supra* note 3, at 198.

Developments in Anonymity

Cryptocurrencies currently face the tension between keeping a user's information confidential and barring double spending. A decentralized system must have a publicly available ledger in order to avoid double spending, such as Bitcoin's block chain. If accessed, however, this transfer information may be exploited by others and diminish anonymity[55].

While most current systems disclose all individual transactions in the public ledger, it is also possible to create a system that uses a zero-knowledge proof in order to validate its interactions. Such a system would generate mathematical proof that all transactions have been valid, without actually disclosing the individual transactions. This system requires a trusted setup and would be open to manipulation by the authors.[56] One of the cryptocurrencies currently pursuing this is Zerocash, a successor to Zerocoin: their development is moving into a direction of distributing the trusted setup to multiple nodes which, assuming that at least one of the nodes destroys the relevant files, make it theoretically secure.[57] The computation of the proof would therefore be so far distributed that a manipulation would not only be statistically improbable, but practically impossible.

Theoretical vs. Practical Implementation

A further problem of anonymity is that, while it may be possible to get a perfectly anonymous system in theory, the implementation will always suffer from use-related insecurity. Considering many people have become comfortable with sharing the details of their lives social media, much of the previously mentioned academic research was able to determine identities based on the user's own posts on twitter and similar media. While a system can attempt to mitigate such disclosures, widespread lack of awareness over what one should or shouldn't do in order to keep one's privacy will necessarily create many points of potential attack.

In the same context, a lot of the currency will necessarily have overlaps with real economies, with many users being neither tech experts, nor

---

[55] *Id*.

[56] Eli Ben-Sasson et al., *SNARKs for C: Verifying Program Executions Succinctly and in Zero Knowledge*, 8043 ADVANCES IN CRYPTOGRAPHY – CRYPTO 2013, 90 (2013).

[57] Ian Miers et al., *Zerocoin: Anonymous Distributed E-Cash from Bitcoin*, IEEE SYMPOSIUM ON SEC. & PRIVACY (2013).

particularly concerned with their privacy.[58] If A and B have used the transaction in order to buy clothing online, which is shipped to their home addresses and has their names and prices associated with it, C's transaction will be far easier to determine. While theoretical anonymity is therefore difficult to achieve, anonymity of a widespread cryptocurrency in practice will be yet another step from it.

Nevertheless, there are many developments towards greater anonymity, many of which seem at least theoretically feasible[59]. While the implementation still seems a number of years, or even decades away, computing capacity is steadily increasing and the cryptologists are learning from many issues with Bitcoin.

POTENTIAL ADJUSTMENTS TO MARIAN'S REGULATORY FRAMEWORK

Challenges to the System

Despite the previously mentioned difficulties, it is within the realm of possibility that a cryptocurrency will be anonymous, or at least difficult enough to crack that it loses feasibility on a large-scale level. If this is on the basis of a zero-knowledge scheme, Marian's concern that there would not be enough trust in the system for it to work would be eliminated, as users would have mathematical proof of the currency's trustworthiness without the need to be able to check the history of transactions.[60] That there can be trust in a system that one does not fully understand is also shown by the large influx of users into the Bitcoin system while it was still widely considered anonymous. While most users were likely not tech experts who would have been able to confirm the trustworthiness themselves, they trusted the perception of its trustworthiness.[61] Consequently, the most extreme scenario would be a trusted currency that would effectively become a black box for outsiders. Any money that is put in disappears to the person not holding the key, and it is impossible to determine the path of the money when it leaves the system.

---

[58] *See* Marian, *supra* note 11, at 67.; *see also*, Monika Taddicken & Cornelia Jers, *The Uses of Privacy Online: Trading a Loss of Privacy for Social Media Gratification?*, *in* PRIVACY ONLINE 143, 143-144 (Sabine Trepte & Leonard Reinecke eds., 2011).

[59] *See generally* Christina Garman, et al., *Rational Zero: Economic Security for Zerocoin with Everlasting Anonymity*, in FINANCIAL CRYPTOGRAPHY AND DATA SECURITY (2014).

[60] *Id*.

[61] Anthony Vance, et al., *Using trust and anonymity to expand the use of anonymizing systems that improve security across organizations*, SEC. J. 1, 11 (2015).

The effect this would have on Marian's proposal is significant: a given user A could earn money through illicit activity and then pay the anonymity tax without fear of any trace to his illicit activity. A bolder user B may earn money through illicit activity, and then claim to have gotten to the level of wealth through fluctuations in the market, effectively avoiding the anonymity tax and simply declaring the money as gains from capital assets. Even at a less extreme level, an otherwise law abiding user C could shift his income from capital gains to ordinary income or reverse without fear of repercussions.

Proposed Adjustments

Input Control Scenario

A potential way of combating this would be to accept the black box scenario, but require all input into the cryptocurrency be declared within a set time frame. This would allow for any tax authority to match declared input to declared output, including time stamps, and reduce the possibility for tax evasion. User C from the previous example would have a declared input, calculated gain or loss, and declared output which can be matched to them. Any discrepancy in output can be put down to undeclared input (if it is higher than expected), saving (if lower), or partial use of the anonymity tax (if lower). The indeterminate state of savings or use of the anonymity tax could be declared by the user at the end of the year, with the savings carrying over. This system would, however, suffer from the potential of a user spending their money through the anonymity tax when speculating for a fall of the currency value, and consequently registering a loss on capital assets that is far greater than what they have actually incurred.

Input and Output Control Scenario

A system that would eliminate privacy but stop users A and B as well, would be to eliminate the elective tax, leading to a requirement to declare input, as well as a requirement to identify oneself when purchasing with cryptocurrency. Since the current way of purchasing things electronically and from a distance is to use a credit card, this is unlikely to diminish privacy over the current state, as the users still have the alternative of paying cash in person. This framework would also be more easily integrated into the existing scheme of income taxation, while the previous example would be a mix of income and consumption tax which would be more difficult to implement.

Crypto-Control Scenario

Finally, it may be possible to further adjust this system as a result of its digital nature, in order to increase the level of anonymity while decreasing the potential for tax evasion and money laundering: Following a users' electronic declaration of input into the black box, the government could issue its own cryptographic token, stating the declared value and timestamp, as well as a cryptographic hash[62] of some means of identifying the users money. The existence of such a token and related adjustment software at the retailer end would allow for someone who opted into this system to pay without disclosing their identity, while giving the retailer confirmation that the money used in the transaction was legitimately declared as income. The software at the retailer end would calculate the amount to be deduced based on a timestamp, and return the token with its diminished value. Once the value of the token runs out, any additional funds that are left over will have to be paid while disclosing one's identity again, as the discrepancy will be due to illicit funds, or capital gains.

Depending on the implementation of such a system parallel to the currency, various degrees of privacy and anonymity could be achieved. For example, it would be possible to disclose more information to the retailers, eliminating privacy at that end, but making it impossible for the government to trace all purchases. Conversely, it may be possible to disclose more information on the government's end, making it possible to trace purchases in general, but allowing for the user to remain unknown to the retailers. Finally, it may even be possible to create a system where it would be possible for the government to access the overall amounts earned and spent by an individual within the currency, without the ability to tell where it was spent. While none of these scenarios would satisfy the state of "being left alone," they would all allow for the user or at least the collective of users, to control which information is accessible by which group of people.

CONCLUSION

The development of cryptocurrencies and their successors will undoubtedly continue into the far future, and regulation of it in order to

[62] In this context, hashing is referring to cryptographic hashing, enabling the shop to verify that the token used is associated with the money being spent, without making it necessary for the government to be informed of the spending, or for the shop to be informed of the amount taxed.

discourage its use as a tool for crime while retaining its advantages will be an ongoing challenge. This literature review outlined the various types of privacy that may be achieved by the technologies used in cryptocurrencies, and determined that it might be possible to satisfy the need for privacy without reaching anonymity. It further considered the current state and developments of anonymity in cryptocurrencies, and concluded that complete anonymity was theoretically possible but far from practical implementation. Looking into Marian's proposed framework for regulation of cryptocurrencies, it was considered what problems the emergence of a blackbox-type cryptocurrency would create for it, and a number of solutions were proposed. Ultimately, the literature review suggested that the technology may be adjusted in tandem with government regulation to serve both society's need for privacy as well as its need to deter criminal activity.

Considering the ongoing development of cryptocurrencies and cryptography in general, as well as the theoretical possibility of unbreakable encryption, it is important to consider the implications of such an occurrence for legislature and regulations. To balance the line between regulation and maintaining privacy, it may also be possible to use the same technologies that are creating the problems in order to aid their regulation.